# ANLEITUNG DG SICHERHEITSPAKET

Einfach sicher surfen.

deutsche-glasfaser.de

Deutsche Glasfaser

# INHALT

# 1 ÜBER DAS DG SICHERHEITSPAKET

Das DG Sicherheitspaket ist eine Softwarelösung, mit der Sie Computer, Smartphones und Tablets von Ihnen und Ihrer Familie schützen können.

Es bietet einen umfassenden Schutz vor Viren, Würmern, Malware, Phishing-Seiten und anderer Schadsoftware in einem Gesamtpaket an.

**Zu den Sicherheitsfeatures gehören:**

- Virenschutz: automatische Erkennung und Entfernung von Viren, Würmern, Malware und anderer Schadsoftware.
- Browser-Schutz: Schutz vor schädlichen und gefährlichen Webseiten.
- Banking-Schutz: Sicherheit beim Online-Banking und/oder bei Geldüberweisungen im Internet inkl. Schutz vor unsicheren Banking-Seiten.
- Suchfunktion für eingebundene Endgeräte: Ortung des Smartphones/Tablets bei Verlust und Verwaltung per Remote-Zugriff über My-Secure.
- Familienmanager: Schutz der Privatsphäre der Kinder und Sperrung von schädlichen Inhalten oder Webseiten sowie Begrenzung der Surfzeit von Familienmitgliedern.
- Gerätefinder: Lokalisierung eines verloren gegangenen Android- oder iOS-Geräts sowie Sperrung oder Löschung per Fernzugriff.

Mit dem Erwerb des DG Sicherheitspakets können Sie je nach Lizenz bis zu fünf Endgeräte schützen. Weitere Informationen finden Sie hier:
**deutsche-glasfaser.de/sicherheitspaket**

# 2 VORAUSSETZUNGEN ZUR NUTZUNG DES DG SICHERHEITSPAKETS

Bevor Sie mit der Einstellung des Sicherheitspakets starten, prüfen Sie bitte, ob folgende Voraussetzungen gegeben sind:

- Sie haben das DG Sicherheitspaket bei Deutsche Glasfaser beauftragt und die gewünschte Lizenzgröße gewählt.
- Ihr Glasfaseranschluss von Deutsche Glasfaser ist bereits technisch aktiv und Sie verfügen über eine Internetverbindung.
- Sie haben für Ihr DG Sicherheitspaket über die Benutzeroberfläche „My-F-Secure“ ein Konto angelegt.
- Ihre Endgeräte erfüllen die Systemvoraussetzungen und sind auf dem neuesten Stand.
- Sie haben keine vergleichbare Software eines anderen Anbieters installiert.
- Sie sind bei Ihrem Computer als Administrator angemeldet.

## 2.1 Anlegen eines Kontos unter „My-F-Secure“

- Nach Beauftragung des DG Sicherheitspakets erhalten Sie eine Willkommens-E-Mail von Deutsche Glasfaser mit einem Installationslink und den Zugangsdaten zur Anmeldung:


Deutsche Glasfaser

Einladung zum DG Sicherheitspaket!

Sehr geehrter Glasfaserkunde,

Max Mustermann hat Sie dazu eingeladen, das DG Sicherheitspaket zu nutzen.

Installieren Sie das Paket jetzt und profitieren Sie noch heute von den umfangreichen Leistungen für ein sorgenfreies Interneterlebnis.

Sie werden eventuell gebeten, sich einzuloggen. Nutzen Sie dafür diese Daten:

E-Mail: Ihr Name
Passwort: Ihr Passwort

Diese E-Mail wurde automatisch für Sie erstellt. Sollten Sie Fragen zu dieser E-Mail oder zum DG Sicherheitspaket haben, kontaktieren Sie uns gerne hier.

Hilfe OK Abbrechen

**Hinweis:** Bitte ändern Sie das initiale Passwort nach der ersten Anmeldung.

- Folgen Sie dem Installationslink und geben Sie Ihre Zugangsdaten ein.
- Nach der Anmeldung werden Sie aufgefordert, ein „persönliches Passwort“ einzugeben, welches Sie für jede weitere Anmeldung verwenden.
- Sobald Sie angemeldet sind, erhalten Sie Zugriff zur Benutzeroberfläche „My-F-Secure“ des DG Sicherheitspakets.
- In der rechten oberen Ecke der Benutzeroberfläche „My-F-Secure“ können Sie die maximal zu vergebenden und noch freien Lizenzen einsehen.

## 2.2 Systemvoraussetzungen zur Nutzung des DG Sicherheitspakets

**Windows**

- Unterstützte Plattformen: Windows 10, 8.1, 8, 7. ARM-basierte Tablets werden nicht unterstützt.
- Prozessor: Intel Pentium 4 oder höher
- Arbeitsspeicheranforderungen: 1 GB oder mehr
- Festplattenspeicher: 1,2 GB freier Festplattenspeicher
- JavaScript muss in den Browsereinstellungen des Benutzers aktiviert sein, um die Sperrseiten aktivieren zu können.

**Mac**

- Unterstützte Plattformen: macOS 10.14 (Mojave) und höher
- Prozessor: Intel
- Arbeitsspeicheranforderungen: 1 GB oder mehr
- Festplattenspeicher: 250 MB freier Festplattenspeicher auf Smartphones und Tablets
- Android 6.0 und höher mit 70 MB freiem Festplatten-speicher
- iOS 12.1 und höher mit 10 MB freiem Speicherplatz auf dem Datenträger
- Sie verfügen über einen aktiven Account für das DG Sicherheitspaket.

## 2.3 Parallele Nutzung von Sicherheitssoftware anderer Hersteller

Bei der Installation des DG Sicherheitspakets wird geprüft, ob noch andere Sicherheitsprogramme mit gleichen Funktionen auf dem Rechner genutzt werden. Diese werden dann deinstalliert, da eine parallele Nutzung nicht möglich ist.

# 3 WIE RICHTE ICH DAS DG SICHERHEITSPAKET AUF MEINEM WINDOWS-RECHNER EIN?

Nachdem Sie einen Account für das DG Sicherheitspaket angelegt haben, können Sie nun über „My-F-Secure“ die beauftragten Lizenzen auf Ihre Endgeräte verteilen und den entsprechenden Software-Client installieren.

**Hinweis:** Stellen Sie die folgenden Dinge sicher:
- Ihr Windows ist auf dem neuesten Stand.
- Sie sind als Administrator angemeldet.
- Sie haben sich bereits mit Ihren Zugangsdaten für das DG Sicherheitspaket registriert.
- Sie verfügen über eine aktive Internetverbindung.

- Sofern Sie nicht mehr über die Benutzerplattform „My-F-Secure“ angemeldet sind, melden Sie sich erneut über den in der Willkommens-E-Mail angegebenen Link an.
- Sobald Sie angemeldet sind, klicken Sie auf den Button **Gerät hinzufügen.**
- Danach öffnet sich ein Fenster mit der Abfrage **Wessen Gerät möchten Sie schützen?.**
- Stellen Sie sicher, dass **Mein Gerät** ausgewählt ist, und bestätigen Sie mit **Fortfahren.** Das Fenster **Gerätetyp wählen** wird geöffnet.
- Stellen Sie sicher, dass **Dieser Computer** ausgewählt ist und klicken Sie auf **Download für Windows.**
- Abhängig von Ihren Browsereinstellungen wird nun die Installationsdatei „automatisch heruntergeladen“ oder Sie werden aufgefordert, die Datei zu speichern.
- Drücken Sie **Strg+J** auf Ihrer Tastatur, um den Downloadordner zu öffnen und die Datei zu suchen.
- Klicken Sie auf die **Installationsdatei** (z. B. F-Secure-Safe-Network-Installer_xxxxxxxxxxxx_.exe), um das Installationsprogramm auszuführen. Wenn das Fenster Benutzerkontensteuerung geöffnet wird, klicken Sie auf **Ja.** Der Setup-Vorgang wird ausgeführt.
- Bestätigen Sie mit **Fortfahren,** wenn die Meldung „Willkommen bei DG Sicherheitspaket“ angezeigt wird.
- Klicken Sie auf **Akzeptieren und fortfahren,** um die Installation zu starten. Wenn Sie anonyme Sicherheitsdaten an die Security Cloud von F-Secure senden möchten, lassen Sie das entsprechende Feld aktiviert.
- Die Installation dauert etwa eine Minute. Sobald die Installation abgeschlossen ist, ist Ihr Computer geschützt.
- Nun können Sie die weiteren Einstellungen im Client vornehmen.

# 4 EINBINDUNG VON ENDGERÄTEN (ANDROID, IOS, MAC)

## Wie richte ich das DG Sicherheitspaket auf meinem Android-Gerät, iOS-Gerät oder auf dem Mac ein?

Sofern Sie nicht mehr bei „My-F-Secure“ angemeldet sind, nutzen Sie den in der Willkommens-E-Mail angegebenen Installationslink und melden Sie sich erneut dort an.

- Klicken Sie auf **Gerät hinzufügen.**
- Danach öffnet sich ein Fenster mit der Abfrage **Wessen Gerät möchten Sie schützen?**
- Stellen Sie sicher, dass **Mein Gerät** ausgewählt ist und klicken Sie auf **Fortfahren.** Das Fenster **Gerätetyp wählen** wird geöffnet.
- Wählen Sie **Anderes Tablet** oder **Anderes Telefon** aus und bestätigen Sie mit **Fortfahren.**
- Wählen Sie entweder **Per E-Mail senden** oder **Per SMS senden** aus, geben Sie die E-Mail-Adresse oder die Telefonnummer ein und klicken Sie auf **Senden,** um den Installationslink des DG Sicherheitspakets an das gewünschte Gerät zu senden.
- Befolgen Sie die Anweisungen in der Nachricht, um das DG Sicherheitspaket zu installieren.

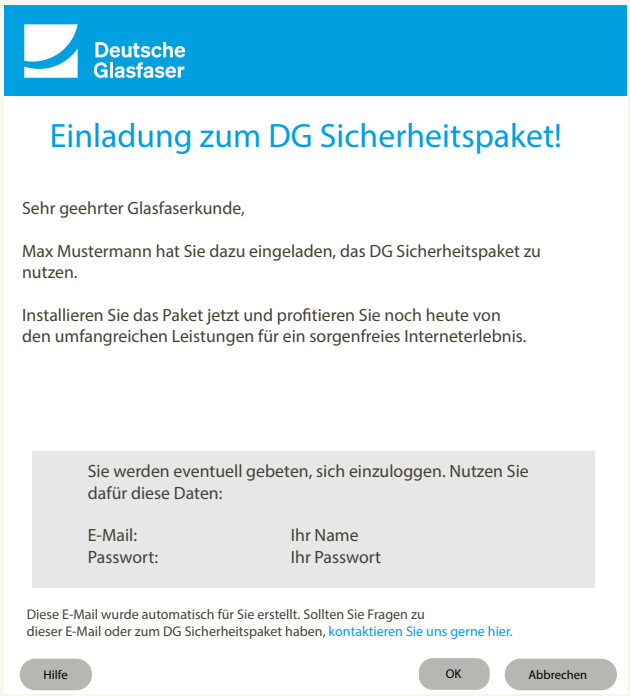

Nehmen Sie jetzt auf dem Android- bzw. iOS-Gerät folgende Einstellungen vor:

- Klicken Sie auf den Link in der SMS-Nachricht oder öffnen Sie Ihren E-Mail-Posteingang und klicken Sie auf die Schaltfläche **Jetzt installieren** in der E-Mail.
- Das DG Sicherheitspaket erkennt automatisch, ob es sich um ein Android-, iOS- oder Mac-Gerät handelt.
- Der Google Play Store bzw. der Apple Store wird geöffnet.
- Bitte installieren Sie die App auf Ihrem Endgerät und akzeptieren Sie die Lizenzbestimmungen.
- Nach der Installation ist Ihr Gerät gesichert.
- Sie können jetzt über den Client die Standard-einstellungen anpassen.

# 5 WEITERLEITUNG EINER FREIEN LIZENZ AN EINEN ANDEREN NUTZER

Sie möchten eine Ihrer freien Lizenzen an ein Familienmitglied oder einen Freund weiterleiten? Dann zeigen wir Ihnen, wie das geht.

- Melden Sie sich über die Benutzeroberfläche Ihres DG Sicherheitspakets an.
- Sobald Sie angemeldet sind, klicken Sie auf **Gerät hinzufügen.** Das Fenster **Wessen Gerät möchten Sie schützen?** wird geöffnet.
- Wählen Sie nicht **Mein Gerät,** sondern **Personengruppe anderer Nutzer.**
- Wählen Sie nun **Benutzer einladen** und klicken Sie auf **Fortfahren.** Das Fenster **Gerätetyp** wählen wird geöffnet.
- Wählen Sie, je nachdem, welches Gerät Sie schützen möchten, **Anderer Computer, Anderes Tablet** oder **Anderes Telefon** aus und klicken Sie auf **Fortfahren.**
- Wählen Sie entweder **Per E-Mail senden** oder **Per SMS senden** aus, geben Sie die E-Mail-Adresse oder die Telefonnummer ein und klicken Sie auf **Senden,** um die Einladungs-E-Mail mit dem Installationslink an das gewünschte Gerät zu senden.
- Öffnen Sie den E-Mail-Posteingang auf dem Endgerät, auf dem das DG Sicherheitspaket noch installiert werden soll, und rufen Sie die Einladungs-E-Mail auf:




Sofern Sie die Einladungs-E-Mail per SMS verschickt haben, öffnen Sie die SMS und folgen Sie den Anweisungen.

Das DG Sicherheitspaket erkennt automatisch, ob es sich um ein Android-, iOS- oder Mac-Gerät handelt.

Bei Mobilgeräten wird der Google Play Store oder der App Store geöffnet. Auf einem PC/Mac wird das Installationsprogramm auf Ihren Computer heruntergeladen.

# 6 EINSTELLUNGEN INNERHALB DER OBERFLÄCHE VON „MY-F-SECURE“

Es gibt vier verschiedene Arten von Clients, die vom DG Sicherheitspaket unterstützt werden:

- Windows-PC
- Mac-PC
- Android-Geräte
- iOS-Geräte

**Hinweis:** Hinsichtlich Design und Funktionen gibt es keinen Unterschied zwischen den Clients. Lediglich die Darstellungsgröße kann abhängig vom genutzten Endgerät abweichen.

**Oberfläche „My-F-Secure“:**
Die folgenden Einstellungen sind über den Software-Client vorzunehmen.

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

**So funktioniert die Security Cloud**
Die Security Cloud sammelt Sicherheitsdaten zu unbekannten Anwendungen und Websites und zu schädlichen Anwendungen und Schwachstellen bei Websites. Wenn Sie die Security Cloud abonnieren, können wir wichtige Informationen sammeln, die wir benötigen, um unsere Sicherheitsdienste bereitzustellen und die Sicherheit unserer anderen Dienste verbessern zu können. Aus diesem Grund und damit unsere Dienste effizient funktionieren, ist es für uns essenziell, Sicherheitsdaten zu unbekannten Dateien, verdächtigem Geräteverhalten oder besuchten URLs zu sammeln. Die Security Cloud verfolgt weder Ihre Webaktivitäten noch sammelt sie Informationen auf Websites, die bereits analysiert wurden. Sie sammelt auch keine Informationen zu sauberen Anwendungen, die auf Ihrem Computer installiert sind. Sicherheitsdaten werden nicht für personalisierte Werbung verwendet. Sie können diese Einstellung später ändern.

## 6.1 Virenschutz

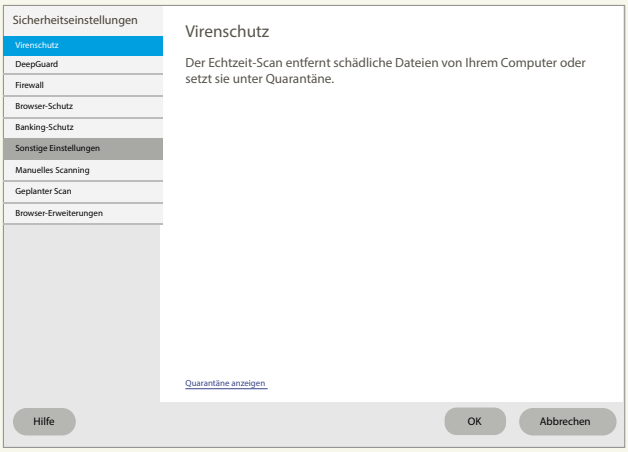
Das Produkt DG Sicherheitspaket schützt den Computer vor Programmen, die möglicherweise persönliche Informationen stehlen, den Computer beschädigen oder ihn für illegale Zwecke einsetzen.

Der Virenschutz bearbeitet standardmäßig alle gefundenen schädlichen Dateien sofort, sodass sie keinen Schaden anrichten können.

Das Produkt scannt alle lokalen Festplatten, Wechseldatenträger (wie z. B. tragbare Laufwerke oder DVDs) und sämtliche heruntergeladenen Inhalte automatisch. Um die Einstellungen zu bearbeiten, können Sie im Client unter dem Reiter **Virenschutz und Einstellungen** die entsprechenden Einstellungen unter dem Punkt **Default** ändern.

**Hinweis:** Sie benötigen Administratorenrechte, um die Einstellungen für den Virenschutz zu ändern.

Wir empfehlen, den Virenschutz stets aktiviert zu lassen, um ungewollten Zugriff auf Ihren Computer zu verhindern. Bei deaktiviertem Virenschutz ist Ihr Computer ungeschützt Schädlingen ausgesetzt.

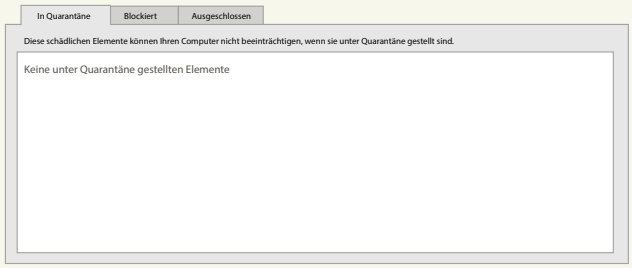



**Einstellungen zur Quarantäne**
Sie können sich aktuell in der Quarantäne befindliche Elemente anzeigen lassen. Diese Elemente können Ihr Endgerät nicht beeinträchtigen.

Die in der Quarantäne befindlichen Elemente können gelöscht oder zugelassen werden. Mit der Einstellung **Zulassen** geben Sie das gefundene Element wieder frei, setzen sich aber eventuell einer Gefahr aus.

Mit der Einstellung **Löschen** werden die Inhalte komplett aus der Quarantäne gelöscht. Das Löschen eines Elements aus der Quarantäne entfernt es endgültig von Ihrem Computer.

**Hinweis:** Über den Reiter **Tools** und **Anwendungs- und Dateisteuerung** kann man sich die Elemente in Quarantäne anzeigen lassen, löschen oder zulassen.




## 6.2 DeepGuard

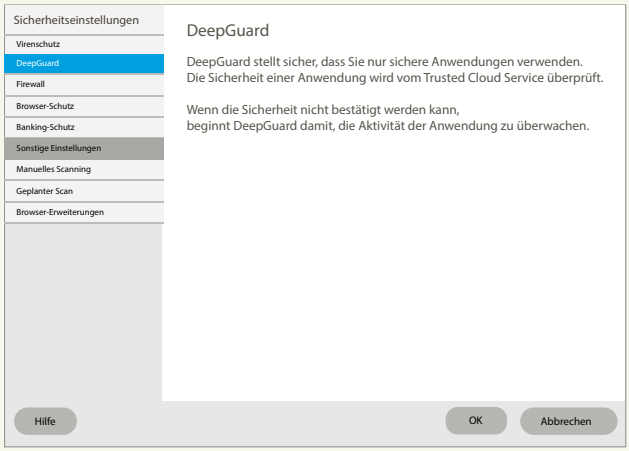
**Begriffserklärung der schädigenden Elemente**

- **Würmer:** sind Programme, die Kopien ihrer selbst von einem Gerät zum nächsten über ein Netzwerk weiterverbreiten. Einige Würmer führen auf betroffenen Geräten auch schädliche Aktionen aus.
- **Trojaner:** sind Programme, die eine interessante oder nützliche Funktion anbieten oder anzubieten scheinen, im Hintergrund dabei jedoch unbemerkt schädliche Aktionen ausführen.
- **Backdoors:** sind Funktionen oder speziell erstellte Programme, die verwendet werden können, um die Sicherheitsvorrichtungen eines bestimmten Programms, Geräts, Portals oder Dienstes zu umgehen. Backdoors werden typischerweise von Angreifern eingesetzt, um nicht autorisierten Zugriff zu erlangen oder schädliche Aktionen auszuführen.
- **Exploits:** sind Objekte oder Methoden, die an der Schwachstelle eines Programms ansetzen, um dessen Verhalten auf unvorhergesehene Weise zu ändern und letztendlich einen Betriebszustand zu erreichen, den Angreifende zu ihrem Vorteil ausnutzen können.
- **Exploit Kits:** sind Toolkits, die Angreifende einsetzen, um Exploits zu verwalten und Schadprogramme auf angreifbare Computer oder Geräte einzuschleusen.

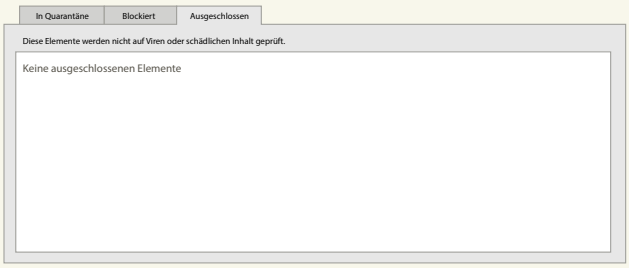
DeepGuard überwacht Anwendungen, um potenziell gefährliche Änderungen für das System zu ermitteln. Es stellt sicher, dass Sie nur sichere Anwendungen nutzen. Die Sicherheit einer Anwendung wird durch den vertrauenswürdigen Cloud-Service verifiziert. Wenn die Sicherheit einer Anwendung nicht verifiziert 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
- Versuche, wichtige Systemdateien zu verändern

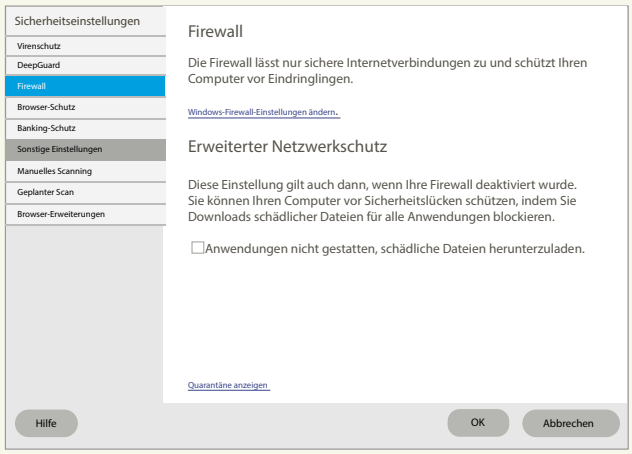



Durch Klicken auf **Ausgeschlossene Dateien anzeigen,** wird folgendes Pop-up angezeigt, in dem die Elemente angezeigt werden, die nicht gescannt werden, weil sie von Ihnen freigegeben wurden.




## 6.3 Firewall

Die Firewall verhindert das Eindringen von Hackern und schädlichen Anwendungen über das Internet in Ihren Computer. Die Firewall lässt nur sichere Internetverbindungen auf Ihrem Computer zu und blockiert unberechtigte Eingriffe über das Internet. Wir empfehlen, die Firewall stets aktiviert zu lassen, um ungewollten Zugriff auf Ihren Computer zu verhindern. Bei deaktivierter Firewall ist Ihr Computer ungeschützt Netzwerkangriffen ausgesetzt. Wenn eine Anwendung nicht mehr funktioniert, weil sie nicht auf das Internet zugreifen kann, deaktivieren Sie keinesfalls die Firewall, sondern ändern Sie die Firewall-Einstellungen entsprechend.



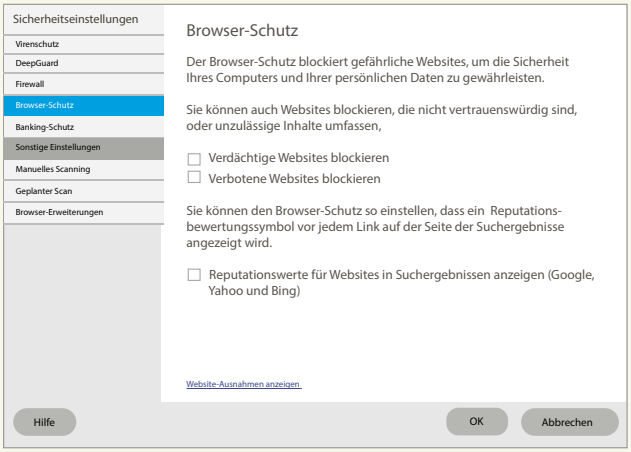

Die Einstellungen sind standardmäßig auf die Verwendung mit der Windows-Firewall eingerichtet. Das Produkt verwendet die Windows Firewall für alle Firewall-Grundfunktionen, wie z. B. die Kontrolle des eingehenden Netzwerkverkehrs und die Trennung Ihres internen Netzwerks vom öffentlichen Internet. Zusätzlich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

**Hinweis zur Verwendung einer persönlichen Firewall:** Wenn Sie die Windows-Firewall durch eine andere Firewall ersetzen, stellen Sie sicher, dass diese einen ein- und ausgehenden Netzwerkverkehr für alle F-Secure-Prozesse zulässt. Ebenso sollte gewährleistet sein, dass Sie die F-Secure-Prozesse zulassen, wenn die Firewall dies anfragt.

## 6.4. Browser-Schutz

Der Browser-Schutz unterstützt Sie und Ihre Familie bei einer sicheren Nutzung des Internets. Er schützt Sie nicht nur vor schädlicher Software und böswilligen Websites, Sie können auch die Inhalte einschränken, die sich Ihre Kinder ansehen können. Zusätzlich können Sie festlegen, wann und wie lange jemand das Internet nutzen darf.

Um die Sicherheit zu verbessern, verwenden mittlerweile viele Websites, beispielsweise Google, einen verschlüsselten Webverkehr mit HTTPS. Dies ist eine gute Initiative und verhindert, dass der Webverkehr eines Benutzers in öffentlichen WLAN-Bereichen (Cafés, Flughäfen usw.) abgefangen werden kann. Der Browser-Schutz schützt den verschlüsselten Webverkehr ebenso wie nicht verschlüsselten Webverkehr. Wenn Sie beispielsweise mit Google eine Suche durchführen, werden Ihnen für jedes Suchergebnis Sicherheitsbewertungen angezeigt. Um diese Funktion zu nutzen, aktivieren Sie nach der Installation die Browser-Schutz-Browser-Erweiterung. Aufgrund der HTTPS-Verschlüsselung müssen Sie die Browser-Erweiterung/das Plug-in für Ihren Browser aktivieren. Diese Funktion ist derzeit in Internet Explorer 7–10, Firefox und Chrome verfügbar.




**Wie aktiviere ich den Browser-Schutz?**
Wenn Sie nach der Installation des DG Sicherheitspakets auf Ihrem PC Ihren Browser das erste Mal öffnen, aktivieren Sie die Browser-Schutz-Erweiterung (Add-on) wie folgt:

- Schieben Sie den Schiebeschalter auf **On.** Der Browser-Schutz von F-Secure ist nun aktiviert.
- Klicken Sie **Verdächtige Websites blockieren** und **Verbotene Websites blockieren.**
- „Verdächtige Website analysiert das System selbst“ muss angekreuzt sein.
- Verbotene Websites werden durch verschiedene Einstellungen, z. B. Inhaltsfilter, etc. blockiert.

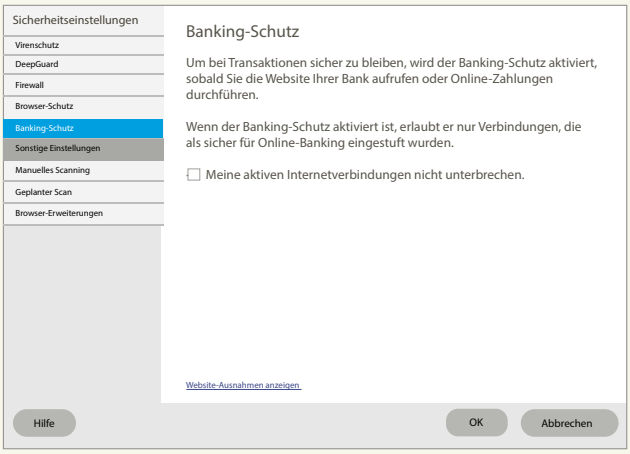
## 6.5 Banking-Schutz

Der Banking-Schutz bietet Ihnen zusätzliche Sicherheit beim Online-Banking und bei Geldüberweisungen im Internet.

Wenn Sie den Banking-Schutz nutzen, wird jede Website, die Sie aufrufen, durch eine Abfrage unserer Security Cloud überprüft. Durch diese Überprüfung erhält der Banking-Schutz Informationen darüber, ob die Website eine von uns als vertrauenswürdig eingestufte Banking-Website ist oder nicht. Wenn die Website als vertrauenswürdig eingestuft wird, wird eine Benachrichtigung angezeigt, dass Sie eine durch HTTPS gesicherte Online-Banking-Website aufrufen und dass der Banking-Schutz zu dem Ergebnis gekommen ist, dass Sie diese Website sicher nutzen können.

Wenn Sie Ihre nächste Online-Banking-Sitzung starten, wird der Banking-Schutz automatisch erneut aktiviert. Anmerkung: Auf Ihrem PC bietet Ihnen der Banking-Schutz zusätzliche Sicherheit. Sobald Sie eine Online-Banking-Sitzung gestartet haben und der Banking-Schutz-Modus aktiviert wurde, trennt der Banking-Schutz alle Verbindungen zu nicht vertrauenswürdigen Anwendungen aus dem Internet und hindert diese daran, sich erneut zu verbinden, solange Sie sich auf einer vertrauenswürdigen Online-Banking-Website befinden. Durch das Blockieren von Verbindungen wird verhindert, dass Ihre Banking-Sitzung gehackt wird. So sind Sie beim Online-Banking stets sicher unterwegs. Zudem können Sie während einer Online-Banking-Sitzung nur auf Websites zugreifen, die als vertrauenswürdig gelten. Als nicht vertrauenswürdig eingestufte Websites werden geblockt.

**Anmerkung:** Wenn Sie die Banking-Schutz-Funktion auf einem Android-Gerät nutzen möchten, verwenden Sie bitte „SAFE-Browser“.




## 6.6 Gerätefinder

Lokalisieren Sie Ihr verloren gegangenes Android- oder iOS-Gerät und sperren oder löschen Sie es per Fernzugriff.

# 7 SONSTIGE EINSTELLUNGEN

Zusätzlich zu den Sicherheitseinstellungen können folgende **Sonstige Einstellungen** vorgenommen werden:

- Manuelles Scanning
- Geplanter Scan
- Browser-Erweiterungen

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

## 7.1 Manuelles Scanning

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

Der Scan des ganzen Computers scannt alle internen und externen Festplatten auf Viren, Spyware und potenziell schädliche Anwendungen. Zudem wird auch nach Elementen gesucht, die möglicherweise von einem Rootkit versteckt werden.

Der Scan des ganzen Computers kann unter Umständen lange dauern. Sie können auch nur einzelne Teile Ihres Systems scannen, die installierte Anwendungen enthalten, um unerwünschte Anwendungen und schädliche Elemente auf Ihrem Computer noch effizienter zu finden und diese zu entfernen.

**Scannen von Dateien und Ordnern**
Wenn Sie befürchten, dass bestimmte Dateien auf Ihrem Computer schädlich sind, haben Sie die Möglichkeit, lediglich diese Dateien zu scannen. Es ist ebenfalls möglich, ganze Ordner und auch externe Festplatten zu scannen.

Diese Scanvorgänge sind deutlich schneller abgeschlossen als ein Scan Ihres gesamten Computers.

## 7.2 Geplantes Scanning

Stellen Sie beispielsweise für die Zeit, in der Sie nicht arbeiten, automatische Scanvorgänge und das Entfernen von Malware oder anderen schädlichen Anwendungen ein. Sie können auch periodische Scanvorgänge planen. So planen Sie einen Scan:

1. Wählen Sie **Weitere Einstellungen** > **Geplantes Scanning.**
2. Aktivieren Sie die Option **Geplanter Scan.**
3. Geben Sie an, wann der Scanvorgang gestartet werden soll.

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

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

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

5. Sie können den Ablauf des geplanten Scanvorgangs auf Ihrem Computer optimieren: Wählen Sie **Scan mit niedriger Priorität starten,** damit der geplante Scanvorgang andere Aktivitäten auf dem Computer weniger beeinflusst und klicken Sie dann auf **OK.** Das Ausführen des Scanvorgangs mit niedriger Priorität dauert länger.

## 7.3 Browser-Erweiterungen

Der Browser-Schutz verwendet Browser-Erweiterungen, um Ihre Sicherheit beim Surfen im Internet zu gewährleisten.

Auf der Seite Virenschutz des Produkts wird angezeigt, wenn die Erweiterung für Ihren Standardbrowser nicht aktiviert ist.

**Wie aktiviere ich die Browser-Schutz-Erweiterung in Firefox oder in Chrome?**
Wenn Sie nach der Installation des DG Sicherheitspakets auf Ihrem PC Ihren Browser das erste Mal öffnen, aktivieren Sie die Browser-Schutz-Erweiterung (Add-on) wie folgt:

- Öffnen Sie Firefox oder Chrome, klicken Sie in der rechten oberen Ecke Ihres Browsers auf die Menüschaltfläche und wählen Sie **Add-ons.**
- Gehen Sie unter **Erweiterungen** zu **Browser-Schutz** von F-Secure und klicken Sie auf **Aktivieren**.

Alternativ können Sie auf **Erweiterung aktivieren** klicken, wenn Sie in der rechten oberen Ecke des Browsers eine Benachrichtigung sehen. Der Browser-Schutz von F-Secure ist nun aktiviert.

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

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

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

# 8 FAMILIENMANAGER-EINSTELLUNGEN

## 8.1 Worum handelt es sich beim Familienmanager?

Der Familienmanager ist eine Funktion innerhalb des DG Sicherheitspakets, mit der Sie die Sicherheit Ihrer Kinder im Internet gewährleisten können. Beim Surfen im Internet kommen Kinder unter Umständen in Kontakt mit ungeeigneten Inhalten, laden versehentlich Malware herunter, die Ihr Gerät beschädigen kann, oder erhalten belästigende Nachrichten nach dem Surfen auf unsicheren Websites.

Mit der Kindersicherung können Sie bestimmte Inhaltstypen blockieren, sodass diese nicht angezeigt werden, wenn Ihr Kind im Internet surft. Sie können auch festlegen, dass Ihr Kind nur Websites aufrufen kann, die Sie vorher ausgewählt haben. Darüber hinaus können Sie nicht jugendfreie Inhalte in Suchergebnissen ausblenden.

Bei der Beschränkung Ihrer Geräte unterscheiden sich die Möglichkeiten je nach Betriebssystem:

**Android:** gesamte Nutzung des Gerätes, außer Anrufen und Textnachrichten
**iPhone und iPad:** Surfen im Internet
**Windows:** gesamte Nutzung des Gerätes

## 8.2 Wie kann ich die Nutzungszeit einschränken?

Diese Einstellungen sind über die Benutzeroberfläche „My-F-Secure“ unter den einzurichtenden Geräten einzurichten.

- Nachdem Sie das Benutzerkonto Ihres Kindes erstellt und ausgewählt haben, klicken Sie auf **Einstellungen.** Wählen Sie unter **Kindersicherung** die Option **Zeitlimits** aus.
- Schieben Sie den Regler nach rechts, um die Funktion zu aktivieren.
- Markieren Sie die Zeiten des Tages, an denen der PC genutzt werden darf. Sie können auch die Anzahl der Stunden begrenzen, für die Ihr Kind den PC nutzen kann, und für Wochentage und Wochenenden unterschiedliche Einstellungen festlegen.
- Klicken Sie auf **OK,** um die Einstellungen zu bestätigen.

## 8.3 Wie kann ich bestimmte Inhalte für mein Kind sperren?

Diese Einstellungen können über die Benutzeroberfläche „My-F-Secure“ unter den einzurichtenden Geräten vorgenommen werden.

- Nachdem Sie das Benutzerkonto Ihres Kindes erstellt und ausgewählt haben, klicken Sie auf **Einstellungen.** Wählen Sie unter **Kindersicherung** die Option **Inhaltsfilter** aus.
  - **a.** Mithilfe der **Inhaltssperre** können Sie Websites je nach deren Inhalt blockieren oder den Zugriff nur auf bestimmte Websites zulassen.
  - **b.** Mit dem **Suchergebnisfilter** werden Google, Yahoo und Bing auf eine strenge Sicherheitsstufe gestellt, sodass nicht jugendfreie Inhalte nicht in den Suchergebnissen angezeigt werden.
- Klicken Sie auf **OK.**

## 8.4 Wie kann ich das Android-Gerät meines Kindes schützen?

Mit den folgenden Einstellungen können Sie auf dem Android-Gerät ein Kinderprofil erstellen und Zeitlimits und Inhaltsfilter für Ihr Kind einrichten.

Senden Sie zunächst einen Installationslink an das Android-Gerät Ihres Kindes. Dies kann von jedem Gerät aus erfolgen, das über eine Internetverbindung verfügt. In diesem Beispiel wird ein PC verwendet:

1. Melden Sie sich bei „My-F-Secure“ mit dem Benutzernamen und Passwort Ihres Kontos an.
2. Sobald Sie angemeldet sind, klicken Sie auf **Gerät hinzufügen.**
3. Wählen Sie **Gerät meines Kindes** aus und klicken Sie auf **Fortfahren.** Wenn Sie ein neues Profil erstellen, klicken Sie auf den **Dropdown-Pfeil** und wählen Sie **Neues Kinderprofil** aus. Klicken Sie auf **Fortfahren.**
4. Wählen Sie aus den Gerätetyp-Optionen **Telefon** aus und klicken Sie auf **Fortfahren.**

5. Wählen Sie aus, wie der Installationslink an das Android-Gerät Ihres Kindes gesendet werden soll.

   a. **Per E-Mail senden**

      - Geben Sie eine E-Mail-Adresse ein, auf die Sie vom Android-Gerät Ihres Kindes aus zugreifen können.
      - Klicken Sie auf **Senden.**

   b. **Per SMS senden**

      - Geben Sie die Telefonnummer Ihres Kindes mit der Landesvorwahl ein.
      - Klicken Sie auf **Senden.**

6. Öffnen Sie nun auf dem Android-Gerät Ihres Kindes die E-Mail oder SMS mit dem Installationslink. Tippen Sie auf den bereitgestellten Link.
7. Klicken Sie auf **Vom App Store installieren.**
8. Klicken Sie auf der Google-Play-Store-Seite von F-Secure SAFE auf **Installieren** und dann auf **Akzeptieren.**
9. Klicken Sie auf **Öffnen.**
10. Lesen und akzeptieren Sie die Nutzungsbedingungen. Klicken Sie auf **Akzeptieren.**
11. Klicken Sie auf der SAFE-Willkommensseite auf **Fortfahren.**
12. Erstellen Sie ein neues Profil für Ihr Kind. Geben Sie den Namen ein und wählen Sie die Altersgruppe aus.
13. Nun können Sie mit Ihrem Kind die Regeln des Familienmanagers durchgehen. Tippen Sie anschließend auf **Weiter.**

    a. **Zeitlimits**

       - Um die Limits für die tägliche Gerätenutzung festzulegen, tippen Sie auf **Bearbeiten** (Stiftsymbol) und schieben Sie den Regler auf die gewünschte Zeitdauer für Wochentage und Wochenenden. Sobald Sie die Einstellungen abgeschlossen haben, klicken Sie auf das **Häkchen-Symbol,** um sie zu speichern.
       - Um die Schlafenszeit festzulegen, tippen Sie auf **Bearbeiten** (Stiftsymbol) und geben Sie die Zeitspanne für Abende vor einem Schultag und für Wochenenden an. Sobald Sie die Einstellungen abgeschlossen haben, klicken Sie auf das **Häkchen-Symbol** und anschließend auf **Weiter.**

    b. **Inhaltsfilter**

       - Wählen Sie durch Aktivieren der Kästchen die Inhaltskategorien aus, die Sie für Ihr Kind blockieren möchten.
       - Klicken Sie auf **Weiter.**

14. Geben Sie im Fenster „Neues Gerät benennen“ einen Namen für das Gerät ein und klicken Sie auf **Fortfahren.**
15. Klicken Sie auf **Weiter.**
16. Für die Funktion „Familienmanager“ werden Geräteadministratorenrechte benötigt, sodass Sie Ihr Kind vor schädlichen Inhalten schützen können. Klicken Sie auf **Fortfahren.**
17. Klicken Sie auf **Diesen Geräteadministrator** aktivieren.
18. Aktivieren Sie die Bedienungshilfen und klicken Sie auf **Fortfahren.**
19. Wählen Sie F-Secure SAFE aus der Liste der Bedienungshilfendienste aus und schieben Sie den Regler in die Position **Ein.**
20. Um F-Secure SAFE zu erlauben, Aktionen zu beobachten und Fensterinhalte abzurufen, klicken Sie auf **OK.**

Das DG Sicherheitspaket ist nun auf dem Android-Gerät Ihres Kindes installiert und die Internetnutzung Ihres Kindes wird gemäß den von Ihnen festgelegten Einstellungen geschützt.

Um die Familienmanager-Einstellungen für das Kind anzuzeigen, tippen Sie auf der App-Startseite auf **Familienmanager.**

Wenn Sie zu einem späteren Zeitpunkt die Familienmanager-Einstellungen ändern möchten, melden Sie sich auf einem beliebigen Gerät in Ihrem My-F-Secure-Konto an und klicken Sie auf das Profil des Kindes, um die Familienmanager-Einstellungen anzuzeigen und zu ändern.

# 9 ALLGEMEINE EINSTELLUNGEN UND PRODUKTBENACHRICHTIGUNGEN

## 9.1 Produktmeldungen anzeigen

In den Produktmeldungen werden Ihnen Benachrichtigungen zu verfügbaren Produkt-Updates und Aktionen angezeigt, die Ihre Aufmerksamkeit erfordern.

So zeigen Sie die Produktmeldungen an:
1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
2 Wählen Sie in dem Pop-up-Menü **Nachrichten anzeigen.**

Die Anzahl der aktuell verfügbaren Nachrichten wird im Pop-up-Menü neben **Nachrichten anzeigen** angezeigt. Die Ansicht mit den Produktnachrichten wird geöffnet und die erste verfügbare Nachricht wird angezeigt.

Wenn Sie eine Lösung zu einer Meldung gefunden haben und auf **Schließen** klicken oder wenn Sie die Meldung zur späteren Bearbeitung zurückstellen, wird die nächste verfügbare Meldung automatisch angezeigt. Wenn keine weiteren Nachrichten mehr vorhanden sind, wird die Meldungsansicht geschlossen.

## 9.2 Verwendung von automatischen Updates

Automatische Updates schützen Ihren Computer vor den neuesten Bedrohungen.

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

**Den Update-Status überprüfen**
Datum und Uhrzeit der letzten Aktualisierung anzeigen.

**Verbindungseinstellungen ändern**
Anweisungen, wie Sie die Art und Weise ändern, wie Ihr Computer Netzwerkverbindungen herstellt und wie Sie mit Updates umgehen möchten, während Sie mobile Netzwerke verwenden.

## 9.3 Anzeige Ereignisse

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

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

So zeigen Sie die Ereignisse an:
1. Klicken Sie mit der rechten Maustaste auf das **Produktsymbol** auf der Taskleiste. Ein Pop-up-Menü wird angezeigt.
2. Klicken Sie in dem Pop-up-Menü auf **Aktuelle Ereignisse anzeigen.** Die Liste der Benachrichtigungen wird geöffnet.
3. Klicken Sie auf **Alle löschen,** wenn Sie alle vorherigen Benachrichtigungen von der Liste entfernen möchten. **Anmerkung:** Diese Aktion kann nicht rückgängig gemacht werden.

## 9.4 Spielmodus

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

- Computerspiele benötigen häufig viele Systemressourcen, um reibungslos zu funktionieren. Andere Anwendungen, die im Hintergrund ausgeführt werden, können die Leistung von Spielen verschlechtern, da sie Systemressourcen und das Netzwerk belegen.
- Der Spielmodus verringert den Einfluss des Produkts auf Ihren Computer und reduziert seine Netzwerkverwendung. Dadurch werden mehr Systemressourcen für Computerspiele freigegeben, während die Grundfunktionen des Produkts unbeeinflusst bleiben. So werden z. B. automatische Updates, geplante Scans und andere Vorgänge ausgesetzt, die viele Systemressourcen und Netzwerkverkehr benötigen.

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

**Spielmodus aktivieren**

1. Klicken Sie mit der rechten Maustaste auf das **Produktsymbol** auf der Taskleiste.
2. Wählen Sie im Pop-up-Menü **Spielmodus.**

Die Nutzung der Systemressourcen durch das Produkt ist nun optimiert und Spiele können auf Ihrem Computer reibungslos ausgeführt werden. Vergessen Sie nicht, den Spielmodus auszuschalten, wenn Sie das Spiel beenden. Der Spielmodus wird automatisch deaktiviert, wenn Sie Ihren Computer neu starten oder den Energiesparmodus verlassen.

Deutsche Glasfaser Wholesale GmbH · Am Kuhm 31 · 46325 Borken
www.deutsche-glasfaser.de · info@deutsche-glasfaser.de
Service-Nr. 02861 890 600
Geschäftsführer: Thorsten Dirks · Guido Eidmann · Angie Hagemann
Jens Müller · Ruben Queimano · Roman Schachtsiek · Christoph Staudt
Sitz der Gesellschaft: Gronau · Amtsgericht: Coesfeld
Registernummer: HRB 14325 · USt-IdNr. DE 287261064
DG_1426_0

Deutsche Glasfaser