DG SICHERHEITSPAKET

Einfach sicher surfen.

deutsche-glasfaser.de

Deutsche Glasfaser

Inhalt

1. Einleitung ... 03

2. Voraussetzungen zur Nutzung des DG Sicherheitspakets ... 04

2.1 Allgemeine Voraussetzungen ... 04

2.2 Systemvoraussetzungen ... 04
Für Windows Computer ... 04
Für Mac Computer ... 04
Für Tablets und Smartphones (Android oder iOS) ... 04

3. Registrierung, Download und Erstinstallation ... 05

3.1 Einrichtung für Windows, Mac, Android oder iOS ... 05

3.2 Erste Schritte – Benachrichtigungen über erforderliche und empfohlene Aufgaben ... 06

3.3 Schutz weiterer Geräte ... 06

3.4 Anzeigen von Informationen zu Ihren Lizenzen ... 07

4. Funktionsweisen der Features ... 08

4.1 Geräteschutz ... 08
Automatischer Scan ... 08
Manueller Scan ... 09
Einstellungen zur Quarantäne ... 10

4.2 DeepGuard ... 11
Begriffserklärung der schädigenden Elemente ... 11

4.3 Firewall ... 12
Verwendung des DG Sicherheitspakets und einer persönlichen Firewall ... 12

4.4 Browser-Schutz ... 13

4.5 Banking-Schutz ... 14
Remote Access Blocker ... 15
Shopping-Schutz ... 15

4.6 Familienmanager ... 16

5. Allgemeine Einstellungen und Produktbenachrichtigungen ... 17

5.1 Produktmeldungen anzeigen ... 17

5.2 Verwendung von automatischen Updates ... 17

5.3 Anzeige von Ereignissen ... 18

5.4 Spielmodus ... 18

1. Einleitung

Unser DG Sicherheitspaket bietet Ihnen umfassenden Schutz sowohl für die Sicherheit Ihrer Geräte als auch für Ihre Privatsphäre und Identität.

Das DG Sicherheitspaket bietet Ihnen:

- Geräteschutz: automatische Erkennung und Entfernung von Viren, Würmern, Malware und anderer Schadsoftware
- DeepGuard: Schutz vor potenziell gefährlichen Anwendungen auf Ihren Geräten
- 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
- Familienmanager: Schutz der Privatsphäre Ihrer Kinder und Sperrung von schädlichen Inhalten oder Webseiten sowie Begrenzung der Surfzeit von Familienmitgliedern

Mit dem Erwerb des DG Sicherheitspakets können Sie je nach Lizenz bis zu fünf Endgeräte schützen.

2. Voraussetzungen zur Nutzung des DG Sicherheitspakets

2.1 Allgemeine Voraussetzungen

Bevor Sie mit der Einstellung des DG 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 Glasfaser-Anschluss von Deutsche Glasfaser ist bereits technisch aktiv und Sie verfügen über eine Internetverbindung.
- Ihre Endgeräte erfüllen die Systemvoraussetzungen und sind auf dem neuesten Stand. Die Systemanforderungen an die unterschiedlichen Geräte finden Sie in Kapitel 2.2.
- Sie haben keine vergleichbare Software eines anderen Anbieters installiert.
- Sie sind bei Ihrem Computer als Administrator angemeldet.

2.2 Systemvoraussetzungen

Für Windows Computer

- Unterstützte Plattformen; Windows 11, Windows 10 mit allen installierten neusten Updates, Windows 8.1. 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 Browser-Einstellungen des Benutzers aktiviert sein, um die Sperrseiten aktivieren zu können.

Für Mac Computer

- Unterstützte Plattformen: macOS 14 (Sonoma), macOS 13 (Ventura), macOS 12 (Monterey)
- Prozessor: Intel oder Apple Silicon
- Arbeitsspeicheranforderungen: 1 GB oder mehr

Für Tablets und Smartphones (Android oder iOS)

- Android Geräte 10.0 und höher mit 70 MB freiem Speicherplatz
- iOS Geräte 17.0 und höher mit 10 MB freiem Speicherplatz
- Festplattenspeicher: 250 MB freier Festplattenspeicher

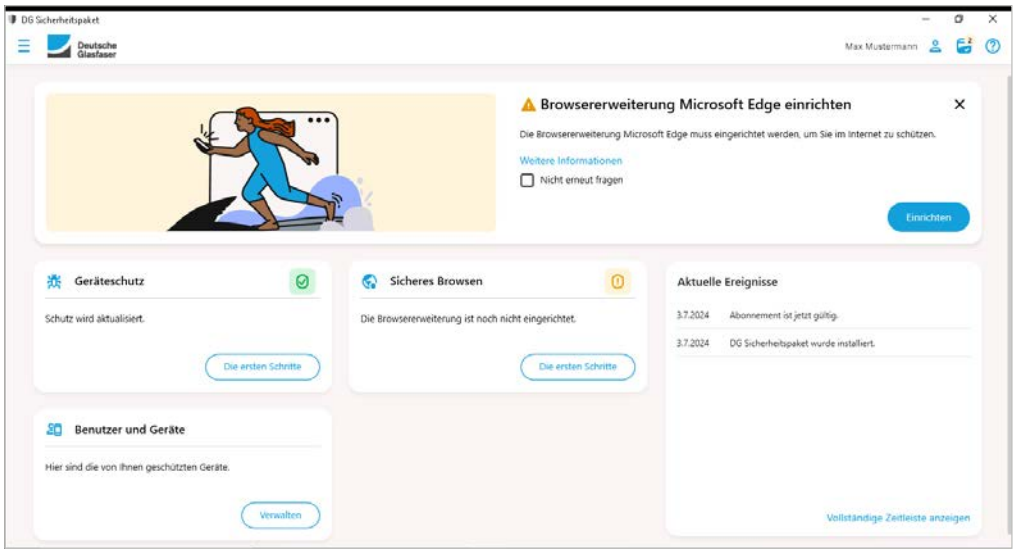
Die aktuellen Systemanforderungen finden Sie auch unter folgendem Link bei unserem Partner f-secure: deutsche-glasfaser.de/dg-sicherheitspaket/systemanforderungen

3. Registrierung, Download und Erstinstallation

3.1 Einrichtung für Windows, Mac, Android oder iOS

Nach Buchung des DG Sicherheitspakets erhalten Sie eine Willkommens-E-Mail von Deutsche Glasfaser mit einem Link zum Download und einem Verifizierungscode. Der Code wird für die Installation des DG Sicherheitspakets benötigt.

Schritt 1	Folgen Sie dem Downloadlink in der E-Mail und laden Sie das DG Sicherheitspaket für Ihr Betriebssystem herunter. Die Anwendung schlägt Ihnen automatisch das für Ihr Gerät passende Betriebssystem vor.
Schritt 2	Die Anwendung öffnet sich auf Ihrem Gerät. Akzeptieren Sie als nächstes die Nutzungsbedingungen.
Schritt 3	Sie werden direkt auf die Startseite des DG Sicherheitspakets weitergeleitet. Nur bei iOS Geräten: Geben Sie den Verifizierungscode aus der Willkommens-E-Mail ein, die Sie von Deutsche Glasfaser erhalten haben. Windows, Mac und Android Geräte benötigen den Verifizierungscode in der Regel nicht.



*Ansicht der **Startseite** des DG Sicherheitspakets auf einem Windows Computer.*
Auf anderen Geräten variiert die Ansicht leicht.

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

3.2 Erste Schritte – Benachrichtigungen über erforderliche und empfohlene Aufgaben

Die Anwendung zeigt Ihnen Aufgaben („Tasks“) an, die Sie erledigen müssen, um den vollständigen Schutz aufrechtzuerhalten. Während bestimmte Aufgaben ein schnelles Handeln verlangen, haben Sie bei anderen zusätzliche Zeit, über die Aufgabe nachzudenken, bevor Sie sie erledigen.

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer, Smartphone oder Tablet.
Schritt 2	Wählen Sie in der Hauptansicht **Alle Tasks** aus.
Schritt 3	Sie sehen eine Übersicht über alle ausstehenden Tasks. Verbessern Sie Ihren Schutz zusätzlich, indem Sie abgelehnte Tasks bearbeiten.

3.3 Schutz weiterer Geräte

Je nach Lizenz können Sie weitere Geräte mit dem DG Sicherheitspaket schützen.

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer, Smartphone oder Tablet.
Schritt 2	Wählen Sie in der Hauptansicht **Benutzer und Geräte** aus.
Schritt 3	Wählen Sie **Gerät hinzufügen.**
Schritt 4	Wählen Sie dann **Mein Gerät.**
Schritt 5	Schicken Sie per E-Mail oder SMS einen Downloadlink und Verifizierungscode an das Gerät, das Sie schützen möchten.
Schritt 6	Öffnen Sie die gesendete E-Mail oder SMS auf dem Gerät, das Sie schützen möchten.
Schritt 7	Folgen Sie dem Downloadlink und Verifizierungscode und laden Sie das DG Sicherheitspaket für Ihren Browser oder Ihr Betriebssystem herunter.
Schritt 8	Sie werden direkt auf die Startseite des DG Sicherheitspakets weitergeleitet. Nur bei iOS Geräten: Geben Sie den Verifizierungscode aus der E-Mail oder SMS ein. Windows, Mac und Android Geräte benötigen den Verifizierungscode in der Regel nicht.

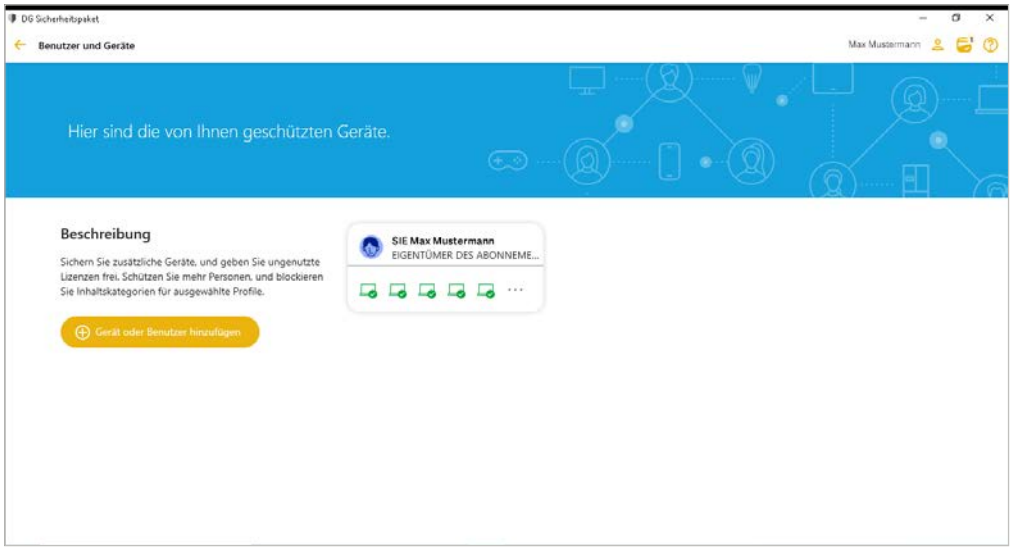


Mit dem Familienmanager können Sie Onlineinhalte für Ihre Kinder beschränken. Weitere Informationen finden Sie in Kapitel 4.6 auf Seite 16.

3.4 Anzeigen von Informationen zu Ihren Lizenzen

Die Verteilung Ihrer Lizenzen können Sie sich in der Anwendung anzeigen lassen.

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer, Smartphone oder Tablet.
Schritt 2	Wählen Sie in der Hauptansicht **Benutzer und Geräte** aus.
Schritt 3	Sie sehen nun die Anzahl der verbliebenen Lizenzen und welche Personen und Geräte über Ihr DG Sicherheitspaket geschützt sind.



*Ansicht der **Übersicht über die DG Sicherheitspaket Lizenzen** auf einem Windows Computer. Auf anderen Geräten variiert die Ansicht leicht.*

Hinweis:
Wie Sie weitere Geräte mit Ihren verfügbaren Lizenzen schützen können, sehen Sie auf S. 6 in Kapitel 3.3.

4. Funktionsweisen der Features

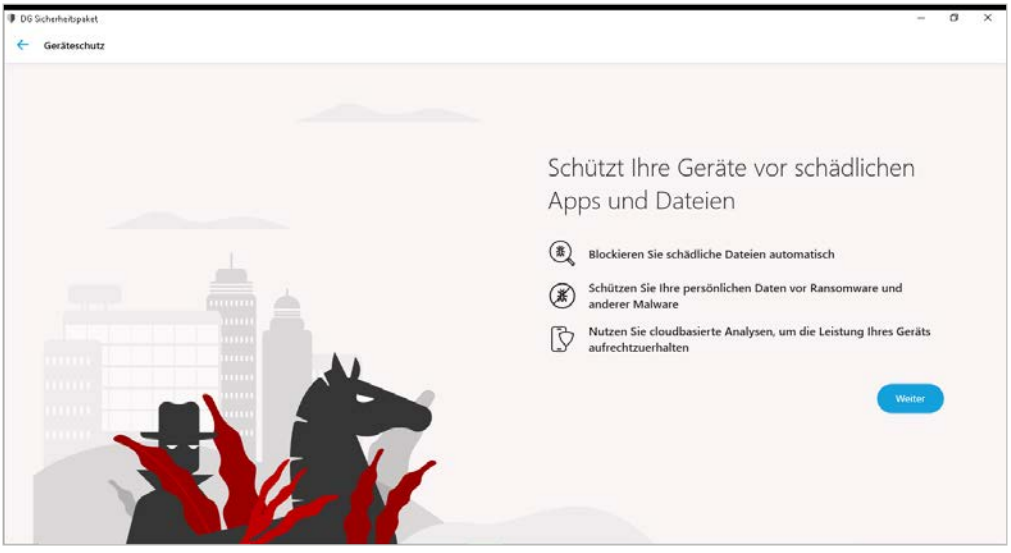
4.1 Geräteschutz

Das DG Sicherheitspaket schützt Computer, Smartphones und Tablets vor Programmen, die möglicherweise persönliche Informationen stehlen, den Computer beschädigen oder ihn für illegale Zwecke einsetzen. Der Geräteschutz bearbeitet standardmäßig alle gefundenen schädlichen Dateien sofort, so dass sie keinen Schaden anrichten können.

Automatischer Scan

So stellen Sie sicher, dass das automatische Scannen aktiviert ist:

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer, Smartphone oder Tablet.
Schritt 2	Wenn in der Hauptansicht des Produkts eine Benachrichtigung angezeigt wird, dass das automatische Scannen deaktiviert ist, wählen Sie **Aktivieren** aus.
Schritt 3	Der Geräteschutz scannt alle lokalen Festplatten, Wechseldatenträger (z. B. tragbare Laufwerke oder DVDs) und sämtliche heruntergeladenen Inhalte automatisch. Um die Einstellungen zu bearbeiten, können Sie in der Anwendung unter dem Reiter **Geräteschutz > Einstellungen** die entsprechenden Einstellungen unter **Default** ändern.



*Ansicht **Geräteschutz** auf einem Windows Computer. Auf anderen Geräten variiert die Ansicht leicht.*

Wir empfehlen, den Geräteschutz stets aktiviert zu lassen, um ungewollten Zugriff auf Ihren Computer zu verhindern. Bei deaktiviertem Geräteschutz ist Ihr Computer ungeschützt Schädlingen ausgesetzt. Wenn beim automatischen Scannen schädliche Inhalte gefunden werden, wird die Datei unter Quarantäne gestellt, bevor sie Schaden anrichten kann (siehe dazu S. 10).

Hinweis:
Sie benötigen Administratorenrechte für Ihr Gerät, um die Einstellungen für den Geräteschutz zu ändern.

Manueller Scan

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

Schritt 1

Öffnen Sie die Anwendung auf Ihrem Computer.

Schritt 2

Wenn Sie den Ablauf des manuellen Scanvorgangs auf Ihrem Computer optimieren möchten, wählen Sie **Geräteschutz > Einstellungen.**

a. Wählen Sie unter **Einstellungen** die Option **Scan-Einstellungen** aus und scrollen Sie nach unten zu **Manueller Scan.**

b. Wählen Sie die Option **Nur Dateitypen scannen, die häufig Schadcode enthalten** (schneller), wenn Sie nicht alle Dateien scannen möchten.

c. Wählen Sie **In komprimierten Dateien scannen** (langsamer), um Dateien zu scannen, die in komprimierten Archivdateien wie z. B. ZIP-Dateien enthalten sind. Durch das Scannen in komprimierten Dateien wird der Scanvorgang verlangsamt. Lassen Sie die Option deaktiviert, um die Archivdatei, aber nicht die darin enthaltenen Dateien zu scannen.

d. Schließen Sie das Fenster **Einstellungen.**

Hinweis:
Bekannte Dateitypen für Schadsoftware sind z. B. Dateien mit den folgenden Erweiterungen: com, doc, dot, exe, htm, ini, jar, pdf, scr, wma, xml, zip.

Schritt 3

Wenn Sie zurück in der Ansicht **Geräteschutz** sind, wählen Sie entweder **Schnell-Scan** oder **Vollständiger Scan des Computers** aus.

a. Beim **Schnell-Scan** werden nur die Systembereiche durchsucht, in denen Anwendungen installiert sind, und anschließend die Speicherorte (einschließlich Ihrer Dokumentenordner), an denen häufig Viren gefunden werden. So werden unerwünschte Anwendungen und schädliche Elemente auf Ihrem Computer in kürzerer Zeit gefunden und entfernt.

b. Mit der Option **Vollständiger Scan des Computers** wird der gesamte Computer mit allen internen und externen Festplatten auf Viren, Spyware und potenziell unerwünschte Anwendungen gescannt. Der vollständige Scan des Computers kann unter Umständen lange dauern.

Der Scanvorgang beginnt. Falls Erkennungen auftreten, werden sie während des Virenscans im Fortschrittskreis angezeigt. Details zu jeder Erkennung werden angezeigt, wenn Sie mit der Maus darauf verharren.

Schritt 4

Die Liste mit möglichen erkannten schädlichen Elementen wird angezeigt.

Schritt 5	Klicken Sie auf das entdeckte Element, um zu entscheiden, wie Sie mit dem schädlichen Inhalt umgehen möchten. **Bereinigen** Dateien automatisch bereinigen. Dateien, die nicht bereinigt werden können, werden unter Quarantäne gestellt. **Quarantäne** Speichern Sie die Dateien an einem sicheren Ort, von dem aus sie nicht andere Dateien infizieren oder Ihren Computer schädigen können. **Löschen** Löschen Sie die Dateien dauerhaft von Ihrem Computer. **Überspringen** Unternehmen Sie vorerst nichts und lassen Sie die Dateien auf Ihrem Computer. **Ausschließen** Die Anwendung darf ausgeführt werden und wird von allen weiteren Scanvorgängen ausgeschlossen.
Schritt 6	Wählen Sie **Alle bearbeiten,** um die Bereinigung zu starten.
Schritt 7	Der Scan zeigt die Endergebnisse und die Anzahl der schädlichen Elemente an, die bereinigt wurden. Nach dem Scan müssen Sie unter Umständen Ihren Computer neu starten, um die Bereinigung abzuschließen. Wenn für die Bereinigung ein Neustart des Computers erforderlich ist, wählen Sie **Neu starten** aus, um das Bereinigen der schädlichen Elemente abzuschließen und den Computer neu zu starten.

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

Einstellungen zur Quarantäne

Sie können sich aktuell in der Quarantäne befindliche Elemente anzeigen lassen. Diese Elemente können Ihr Endgerät nicht beeinträchtigen. Über den Reiter **Tools und Anwendungs- und Dateisteuerung** kann man sich die Elemente in Quarantäne anzeigen lassen, diese löschen oder zulassen. 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.

4.2 DeepGuard

DeepGuard überwacht Anwendungen, um potenziell gefährliche Änderungen für das System zu ermitteln. Es sorgt dafür, dass Sie nur sichere Anwendungen nutzen.

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

So stellen Sie sicher, dass DeepGuard aktiviert ist:

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer.
Schritt 2	Wenn in der Hauptansicht der Anwendung eine Benachrichtigung über deaktivierte Schutzfunktionen angezeigt wird, wählen Sie **Alles aktivieren aus.** Um genauere Informationen zu den deaktivierten Schutzfunktionen zu erhalten, wählen Sie **Weitere Informationen ...** aus.
Schritt 3	Wenn Sie die Benachrichtigung auf der Hauptseite des Produkts verpassen, können Sie alle Schutzfunktionen in der Ansicht Geräteschutz aktivieren, indem Sie **Geräteschutz > Alles aktivieren** auswählen. Wenn Sie einige der Schutzfunktionen bewusst deaktiviert haben, die Risiken verstehen und die Benachrichtigung nicht erneut sehen möchten, wählen Sie **Nicht erneut fragen** aus.
Schritt 4	Sie können auf die Einstellungen von DeepGuard auch über die Produkteinstellungen zugreifen, indem Sie **Geräteschutz > Einstellungen** auswählen.

Info:
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.

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 zu schleusen.

4.3 Firewall

Eine Firewall verhindert das Eindringen von Hackern und schädlichen Anwendungen über das Internet in Ihren Computer. Sie lässt nur sichere Internetverbindungen auf Ihrem Computer zu und blockiert unberechtigte Eingriffe über das Internet.

Das DG Sicherheitspaket enthält keine eigene Firewall. Auf Windows Computern ist die Microsoft Defender Firewall standardmäßig installiert. Auf macOS Geräten müssen Sie die Firewall hingegen manuell in den Einstellungen aktivieren. Weder Smartphones, die mit Android laufen, noch iPhones mit dem iOS Betriebssystem haben eine eigene Firewall installiert. Wählen Sie für ihren Schutz unbedingt einen Drittanbieter aus, dem Sie vertrauen.

Wir empfehlen, eine Firewall stets aktiviert zu lassen. Bei deaktivierter Firewall ist Ihr Computer ungeschützt Netzwerkangriffen ausgesetzt.

Verwendung des DG Sicherheitspakets und einer persönlichen Firewall

Stellen Sie bei der Verwendung einer anderen Firewall sicher, dass diese einen ein- und ausgehenden Netzwerkverkehr für alle DG Sicherheitsprozesse zulässt. Ebenso sollte gewährleistet sein, dass Sie die DG Sicherheitsprozesse zulassen, wenn die Firewall dies anfragt.

4.4 Browser-Schutz

Der Browser-Schutz unterstützt Sie 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 dürfen. Zusätzlich haben Sie die Möglichkeit festzulegen, wann und wie lange jemand das Internet nutzen darf.

So richten Sie die Browser-Erweiterung für Chrome, Edge und Firefox ein:

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer.
Schritt 2	Wählen Sie in der Hauptansicht die Option **Sicheres Browsen** aus.
Schritt 3	Wählen Sie die Option **Einstellungen** aus.
Schritt 4	Navigieren Sie auf der Seite **Sicheres Browsen** zu **Browser-Erweiterungen.**
Schritt 5	Wählen Sie unter **Browser-Erweiterungen** die Option **Add-ons für Ihren Browser** aus.
Schritt 6	Die Seite für die Erweiterung des Browserschutz von F-Secure (unserem Technologiepartner) wird geöffnet.
Schritt 7	Wählen Sie **Abrufen > Erweiterung hinzufügen.**
Schritt 8	Wenn die Erweiterung bereits im Browser installiert, aber deaktiviert wurde, wählen Sie **Einschalten,** um sie zu aktivieren. Sie können jetzt sicher mit Ihrem Browser im Internet surfen.

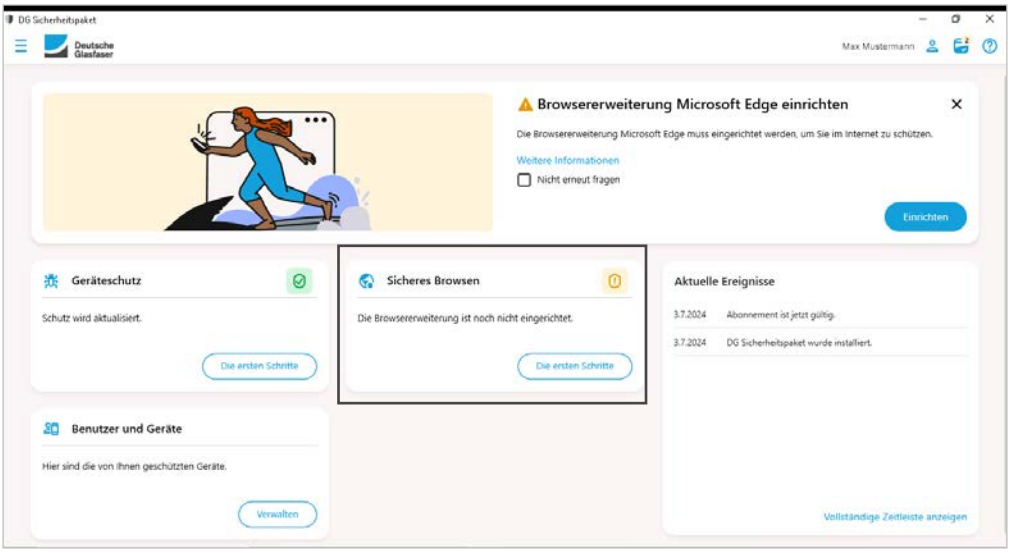
Info:
Um die Sicherheit zu verbessern, verwenden mittlerweile viele Websites (beispielsweise Google) einen verschlüsselten Webverkehr mit HTTPS. Dies ist eine gute Initiative und verhindert, dass der Webverkehr eines Benutzers in öffentlichen WLAN-Bereichen (Cafés, Flughäfen usw.) abgefangen werden kann. Der Browser-Schutz ist derzeit im Internet Explorer 7–10, in Firefox und Chrome verfügbar.

4.5 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, mit einer 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 eine Website vom Browser-Schutz als vertrauenswürdig eingestuft wird, wird eine Benachrichtigung angezeigt, dass Sie eine durch HTTPS gesicherte Online-Banking-Website aufrufen.

Der Banking-Schutz ist standardmäßig aktiviert. Wenn er nicht aktiviert ist, aktivieren Sie den Banking-Schutz wie folgt (am Beispiel eines Windows Computers):

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer.
Schritt 2	Wählen Sie in der Hauptansicht die Option **Sicheres Browsen** aus.
Schritt 3	Wählen Sie die Option **Einstellungen** aus.
Schritt 4	Wählen Sie **Einstellungen bearbeiten.**
Schritt 5	Aktivieren Sie den **Banking-Schutz.**



*Ansicht der **Startseite** auf einem Windows Computer. Auf anderen Geräten variiert die Ansicht leicht.*

Anmerkung:
Als Voraussetzung für den Banking-Schutz müssen Sie die **Erweiterung des Browser-Schutzes** in Ihrem Webbrowser aktivieren (siehe S. 13).

So passen Sie die Banking-Schutzeinstellungen an:

Schritt 1	Deaktivieren Sie die Option **Verbindung für nicht vertrauenswürdige Apps trennen,** wenn der Banking-Schutz Ihre bereits geöffneten Verbindungen nicht schließen soll. Wenn Sie die Einstellung aktiviert lassen, schließt der Banking-Schutz Ihre bestehenden Internetverbindungen bis auf vertrauenswürdige Apps.
Schritt 2	Wenn Sie ein externes Tool verwenden müssen, das während einer Banking-Schutzsitzung gesperrt wird, deaktivieren Sie die Option **Verbindung mit Befehlszeilen- und Skripterstellungstools aufheben.**
Schritt 3	Wählen Sie aus, wie der Banking-Schutz Daten behandeln soll, die in Ihre Zwischenablage kopiert wurden. Standardmäßig ist **Zwischenablage nach Banking-Sitzungen löschen** aktiviert und der Banking-Schutz löscht nach dem Ende Ihrer Banking-Schutzsitzung alle Daten aus der Zwischenablage, um Ihre vertraulichen Daten zu schützen. Deaktivieren Sie diese Einstellung, wenn der Banking-Schutz die Zwischenablage nicht löschen soll.
Schritt 4	Standardmäßig ist der Fernzugriff auf Ihr Gerät während Ihrer Banking-Sitzung blockiert. Banking-Transaktionen sind immer privat und vertraulich und Sie sollten sich **niemals bei Ihrer Online-Bank anmelden, wenn jemand Fernzugriff (Remote-Zugriff) auf Ihr Gerät hat.**

Anmerkung:
Wir empfehlen Ihnen, die Einstellung **Verbindung mit Befehlszeilen- und Skripterstellungstools aufheben** aktiviert zu lassen, sofern eine Deaktivierung nicht absolut notwendig ist, da einige Malware-Angriffe integrierte Windows Komponenten wie PowerShell verwenden können. Dies gibt den Angreifern die Möglichkeit, Zugriff auf Ihre Bankdaten und personenbezogenen Daten zu erhalten.

Wichtig:
Aktivieren Sie nicht die Einstellung **Remote-Zugriff**, sofern Sie nicht sowohl die den Zugriff anfordernde Person als auch den genauen Zweck der Anfrage kennen.

Remote Access Blocker

Während Ihrer Online-Banking-Sitzung erhalten Sie möglicherweise eine Warnmeldung, dass jemand versucht, aus der Ferne auf Ihr Gerät zuzugreifen. Der Remote Access Blocker fügt Ihren Online-Banking-Sitzungen eine weitere Schutzfunktion hinzu: Wenn bei eingeschaltetem Banking-Schutz eine aktive Fernzugriffsverbindung zu Ihrem Gerät erkannt wird, wird diese Verbindung vom Remote Access Blocker sofort unterbrochen.

Shopping-Schutz

So schalten Sie **Shopping-Schutz** aus oder ein:

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer.
Schritt 2	Wählen Sie in der Hauptansicht die Option **Sicheres Browsen** aus.
Schritt 3	Wählen Sie in der Ansicht **Sicheres Browsen** die Option **Einstellungen** aus.
Schritt 4	Wählen Sie **Einstellungen bearbeiten.**
Schritt 5	Schalten Sie **Shopping-Schutz** ein oder aus.
Schritt 6	Aktivieren oder deaktivieren Sie **Benachrichtigungen für sichere Shopping-Websites anzeigen** und **Benachrichtigungen für verdächtige Shopping-Websites anzeigen,** je nachdem, welche Benachrichtigungen Sie sehen möchten.

Info:
Shopping-Schutz macht Ihre Einkäufe im Internet sicherer, indem es Sie über gefälschte und nicht vertrauenswürdige Websites informiert.

Für **Shopping-Schutz** ist es erforderlich, dass die Erweiterung des Browser-Schutzes in dem von Ihnen verwendeten Webbrowser aktiviert ist (siehe dazu S. 13).

4.6 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 dem Familienschutz können Sie für Ihre Kinder den Zugriff auf unangemessene Inhalte einschränken, um zu verhindern, dass sie unerwünschtem Material im Internet ausgesetzt sind.

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

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

Mit der Inhaltsfilterung können Sie die Arten von Onlineinhalten einschränken, auf die Ihr Kind zugreifen kann.

So richten Sie den Schutz für Ihr Kind ein:

Schritt 1	Bevor Sie den Inhaltsfilter über Ihr Gerät steuern können, müssen Sie zunächst das DG Sicherheitspaket auf dem Gerät Ihres Kindes installieren. Folgen Sie dazu der Anleitung in Kapitel 3.3 Schutz weiterer Geräte auf Seite 6.
Schritt 2	Nach der erfolgreichen Installation des DG Sicherheitspaket auf dem Gerät Ihres Kindes, öffnen Sie die Anwendung auf Ihrem Computer, Smartphone oder Tablet.
Schritt 3	Wählen Sie in der Hauptansicht **Familienschutz** aus. Dadurch werden die Einstellungen für den **Familienschutz** geöffnet.
Schritt 4	Wählen Sie **Einstellungen bearbeiten**.
Schritt 5	Wählen Sie das Konto aus, das Sie bearbeiten möchten.
Schritt 6	Aktivieren Sie die **Inhaltsfilterung**.
Schritt 7	Wählen Sie das Inhaltsfilterungsprofil aus. Sie können zwischen **Streng**, **Mäßig** und **Einfach** wählen. Jedes Profil blockiert einen anderen Satz von Inhaltstypen. Wenn die Liste der Inhaltstypen nicht angezeigt wird, scrollen Sie nach unten zur Übersicht der blockierten Inhaltstypen. Sie können auch bestimmte Websites zulassen, selbst wenn diese aufgrund ihres Inhaltstyps von der Inhaltsfilterung blockiert würden: a. Wählen Sie **Website-Ausnahmen anzeigen**. Dadurch wird eine neue Ansicht geöffnet, in der die Websites aufgelistet sind, die Sie zulassen möchten. b. Wählen Sie **Neue hinzufügen**. c. Geben Sie die Adresse der Website ein, die Sie zulassen möchten. d. Wählen Sie **OK**.
Schritt 8	Lassen Sie die VPN-Konfigurationen zu.

Sie haben nun die Inhaltsfilterung für Ihr Kind eingerichtet. Um diese Einstellungen später zu ändern, wählen Sie in der Hauptansicht der App **Familienschutz**.



Sie können die Einstellungen für die Inhaltsfilterung für jedes Benutzerkonto getrennt bearbeiten.

5. Allgemeine Einstellungen und Produktbenachrichtigungen

5.1 Produktmeldungen anzeigen

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

So lassen Sie sich die Produktmeldungen anzeigen (am Beispiel eines Windows Computers):

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

5.2 Verwendung von automatischen Updates

So können Sie sich Details der neuesten Updates für das installierte Produkt anzeigen lassen:

Schritt 1	Öffnen Sie die Anwendung auf Ihrem Computer, Tablet oder Smartphone.
Schritt 2	Wählen Sie in der Hauptansicht oben links die **Menütaste** neben dem DG Logo.
Schritt 3	Wählen Sie **Einstellungen.**
Schritt 4	Wählen Sie unter Einstellungen **Updates.** Unter **Verbindung** sehen Sie den Zeitpunkt der letzten Update-Prüfung und deren Status.
Schritt 5	Wenn Sie manuell nach den neuesten Updates suchen möchten, wählen Sie die Option **Jetzt prüfen.** Bei dieser Prüfung wird auch ein Update auf die neueste Version des DG Sicherheitspakets durchgeführt.



Hinweis:
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.

5.3 Anzeige von Ereignissen

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.

So lassen Sie sich die Ereignisse anzeigen (am Beispiel eines Windows Computers):

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

5.4 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 DG Sicherheitspakets 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 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.

So aktivieren Sie den Spielmodus:

Schritt 1	Klicken Sie mit der rechten Maustaste auf das **Produktsymbol auf der Taskleiste.**
Schritt 2	Wählen Sie im Pop-up-Menü **Spielmodus.**
Schritt 3	Die Nutzung der Systemressourcen durch das Produkt ist nun optimiert und Spiele können auf Ihrem Computer reibungslos ausgeführt werden.
Schritt 4	Vergessen Sie nicht, den Spielmodus auszuschalten, wenn Sie das Spiel beenden.
Schritt 5	Der Spielmodus wird automatisch deaktiviert, wenn Sie Ihren Computer neu starten oder den Energiesparmodus verlassen.

Haben Sie Fragen?

Kontaktieren Sie uns gerne.



Per Telefon:
02861 8906 00



Online über unser Kundenportal:
kundenportal.deutsche-glasfaser.de/service

© 2024 Deutsche Glasfaser Wholesale GmbH.

Alle Rechte vorbehalten.

Betriebsanleitungen, Handbücher und Software sind generell urheberrechtlich geschützt. Das Kopieren, Vervielfältigen, Übersetzen oder Umsetzen in jedwedes elektronische Medium oder in eine maschinell lesbare Form im Ganzen oder in Teilen ist ohne vorherige schriftliche Genehmigung von Deutsche Glasfaser nicht gestattet.

Diese Anleitung wurde mit großem Engagement erstellt, um sicherzustellen, dass die in diesem Handbuch aufgeführten Informationen korrekt sind. Deutsche Glasfaser kann jedoch keine Gewähr für die Richtigkeit des Inhaltes dieser Bedienungsanleitung übernehmen.

DG_1426_7

Deutsche Glasfaser Wholesale GmbH
Kontakt: 40463 Düsseldorf (Postanschrift)