Ratgeber

WLAN Experten-Guide

Wie sichere ich meinen WLAN-Router bestmöglich ab?

SYNVIA hilft.

Sie haben Ihren WLAN-Router erfolgreich eingerichtet und in Betrieb genommen. Herzlichen Glückwunsch! Jetzt kommt der nächste Schritt: die optimale Konfiguration.

WLANs sind verwundbare Netze. Denn sie kommunizieren über Funkwellen, die auch außerhalb Ihrer Räumlichkeiten abgehört werden können. Dadurch besteht einerseits die Gefahr, dass Ihre Internetaktivitäten überwacht werden, andererseits können sich Fremde Zugang zu Ihrem WLAN verschaffen und dort Schaden anrichten.

Dieser Expertenratgeber hilft Ihnen dabei, Ihren WLAN-Router sicher zu machen und die maximale Leistung aus ihm herauszuholen.

Inhaltsverzeichnis

Auf die Benutzeroberfläche des Routers zugreifen

Alle Maßnahmen, die in diesem Leitfaden beschrieben werden, führen Sie an der Benutzeroberfläche Ihres WLAN-Routers durch. Alle Tipps funktionieren mit der **FRITZ!Box**, viele auch mit dem Standard-Kabelmodem Arris, also allen Routern, die SYNVIA einsetzt.

Die Benutzeroberfläche des Routers erreichen Sie von Ihrem Computer aus, entweder über WLAN oder über eine direkte LAN-Verbindung (Kabel) zwischen dem Router und Ihrem Notebook oder PC.

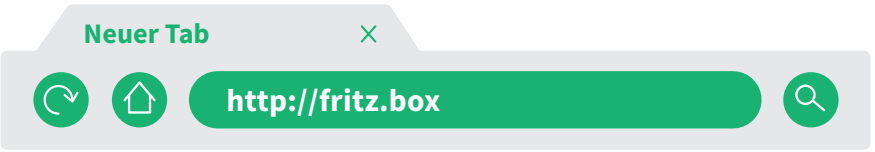
Für den Zugriff benötigen Sie die beiden folgenden Informationen, die Sie im Handbuch oder auf der Unterseite Ihres Routers finden.

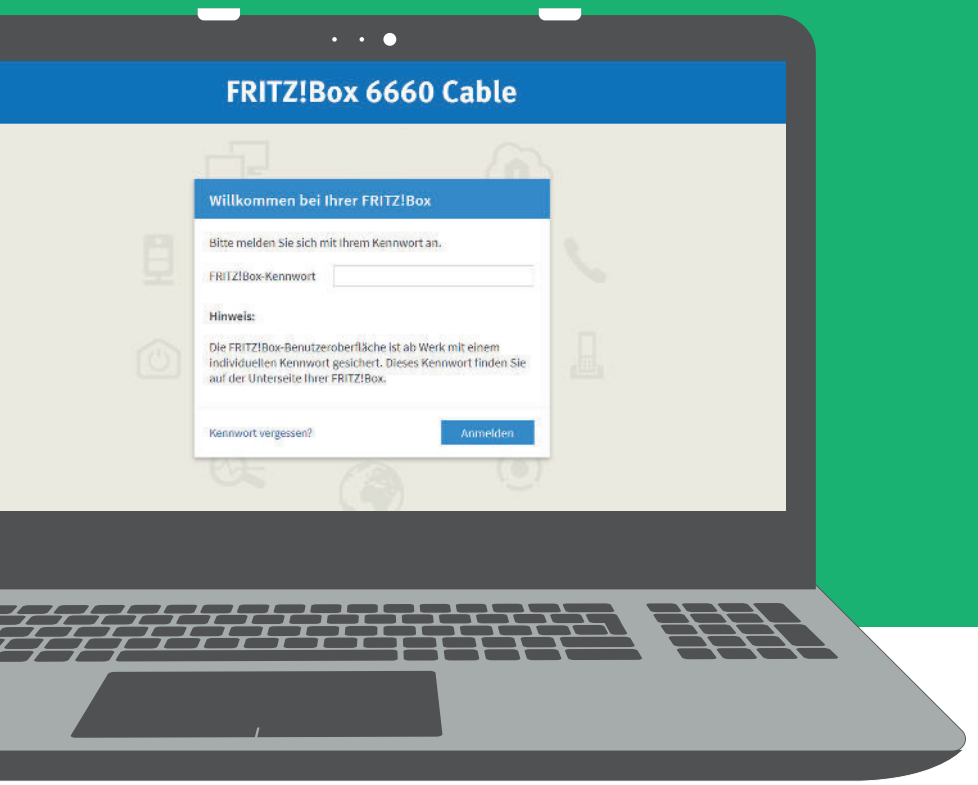
1. Die IP-Adresse oder Internet-Adresse des Routers

Um auf die Benutzeroberfläche der FRITZ!Box zu gelangen, geben Sie in die Adresszeile Ihres Browsers eine der folgenden Befehle ein:

Die Adresse **http://fritz.box**; die IP-Adresse **http://192.168.178.1**; die IP-Adresse **http://169.254.1.1** (Notfall-IP der FRITZ!Box)

Das Standardkabelmodem Arris TG3442 verbinden Sie via LAN-Kabel mit Ihrem Computer und geben die IP-Adresse 192.168.0.1 in den Internetbrowser ein.





2. Das Kennwort

Das bei Auslieferung des Routers voreingestellte Passwort finden Sie im Handbuch oder auf der Unterseite des Gerätes.

Tipp: Häufig sind bei Routern die Zahlen 0000 oder 1234 als Initialpasswort eingestellt. Manchmal reicht es auch, das Passwortfeld leer zu lassen, wenn kein Passwort voreingestellt ist.

Manche Geräte verlangen zusätzlich zum Passwort noch einen Benutzernamen, der oft „Administrator“ oder ähnlich lautet.

Den Gerätezugriff absichern

Router sind im Auslieferungszustand noch nicht ausreichend gesichert. Wenn ein Standardpasswort wie „1234“ voreingestellt ist, braucht man keine Hackerqualitäten, um sich Zugang zu verschaffen.

Sichern Sie daher als Erstes den Zugang zur Benutzeroberfläche ab, indem Sie **das Kennwort ändern.**

Tipp: Dieses Kennwort für den Zugriff auf die Benutzeroberfläche des Routers ist nicht identisch mit dem Kennwort für den Zugriff auf das WLAN!

- Kennwort für die Benutzeroberfläche: Nur für den Administrator (das sind Sie)
- Kennwort für den WLAN-Zugang (WLAN Netzwerkschlüssel): Für alle Nutzer des WLAN

Wenn Sie von außen über das Internet auf Ihren Router zugreifen möchten, müssen Sie einen **Fernzugriff über VPN** (Virtual Private Network) einrichten. Eine Anleitung dazu finden Sie im Handbuch der FRITZ!Box unter „VPN-Fernzugriff einrichten“.

3. Tastensperre

Wenn Sie verhindern möchten, dass Unbefugte den Router bedienen, können Sie die Tastensperre aktivieren. Wählen Sie dazu „System > Tasten und LEDs > Tastensperre“ und aktivieren Sie die Option „Tastensperre aktivieren“.

Nun sind die Tasten zum Ein- und Ausschalten des WLAN und der WPS deaktiviert.

SSID und Netzwerk-schlüssel einrichten

1. Eine eigene SSID vergeben

Der Netzwerkname (SSID) ist ebenfalls voreingestellt. Sie sollten ihn **ändern**, damit Sie und alle anderen Nutzer Ihres WLANs das Netzwerk in der WLAN-Liste ihres Endgerätes leicht finden können. Außerdem vermeiden Sie so, dass sich in Ihrer Umgebung weitere WLANs mit der gleichen SSID befinden, was dazu führen kann, dass Endgeräte versuchen, sich am falschen Router einzuloggen.

Tipp: Wählen Sie keinen Netzwerknamen, der direkt auf Ihre Identität schließen lässt. Denn in diesem Fall kann jede fremde Person sofort erkennen, welches Ihr persönliches WLAN ist. Vergeben Sie einen **einprägsamen Fantasienamen** wie beispielsweise „Jupiter“, „Zwerghase“ oder „Orchidee“.

Sie können für die beiden Funknetze **2,4 GHz und 5 GHz** unterschiedliche SSIDs vergeben. Damit der Router automatisch die für Sie beste Frequenz auswählen kann, sollten Sie dies jedoch nicht tun, sondern die Option „Unterschiedliche Benennung der Funknetze auf 2,4 und 5 GHz“ bei der FRITZ!Box deaktivieren.

2. SSID verstecken

Theoretisch können Sie Ihre SSID auch verbergen. Deaktivieren Sie dazu bei der Vergabe des Netzwerknamens die Option „WLAN-Name sichtbar“. Nun wird Ihr Netzwerk nicht mehr in der WLAN-Liste der Endgeräte angezeigt – Benutzer müssen die SSID kennen und eingeben, um Zugang zu erhalten.

So sicher diese Maßnahme auch klingt, **wir raten davon ab.** Denn Ihr Netzwerk ist zwar unsichtbar, kann aber trotzdem mit entsprechenden Programmen gefunden werden. Die Sicherheit ist also trügerisch und macht Ihren WLAN-Nutzern nur das Leben schwer.

3. Sicherer WLAN-Netzwerkschlüssel

Der WLAN-Netzwerkschlüssel ist das Passwort, das Benutzer eingeben müssen, um auf das WLAN zugreifen zu können, wenn das WLAN mit Verschlüsselung arbeitet (siehe Abbildung auf Seite 8). Das voreingestellte Kennwort ist nicht sicher, da es – je nach Hersteller – für mehrere Geräte verwendet wird. Deshalb sollten Sie dieses Kennwort ändern.

Denken Sie sich ein Passwort für den WLAN-Zugang aus, das nicht zufällig erraten werden kann. Zudem sollten Sie auf Namen, Geburtstage oder andere leicht zu erratene Begriffe verzichten. Wählen Sie am besten eine zufällige Kombination aus Buchstaben, Zahlen und Sonderzeichen.

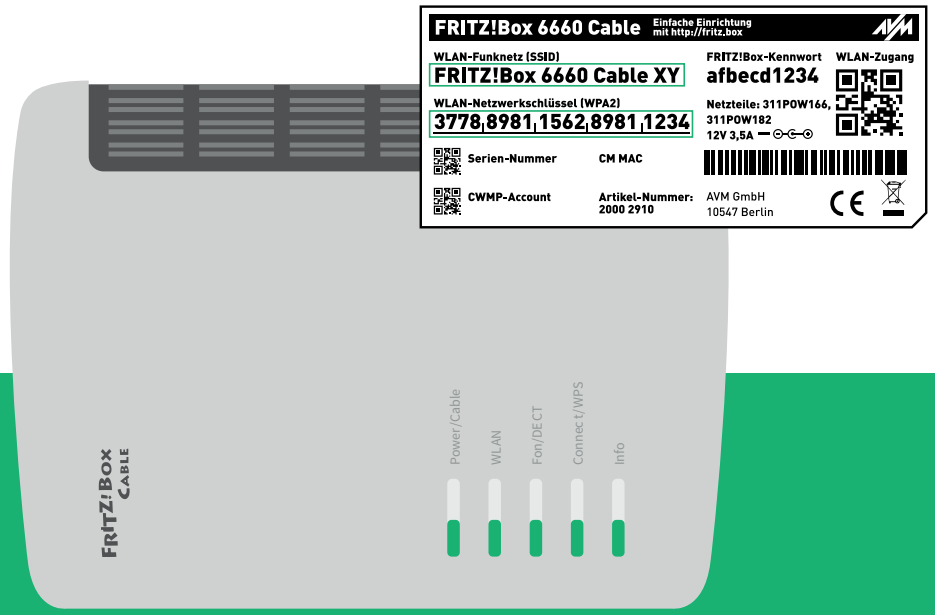
Berücksichtigen Sie dabei, dass das Kennwort auch auf Geräten eingegeben werden muss, die keine komfortable Tastatur haben (z.B. Set-Top-Box): Wählen Sie also kein extrem langes Kennwort; 10 bis 15 Zeichen reichen aus.

Notieren Sie den eingegebenen Netzwerkschlüssel an einem sicheren Ort.

Tipp: Lange Passwörter bleiben natürlich nicht so leicht im Gedächtnis. Mit einem kleinen Trick klappt es aber doch: Denken Sie sich einen Satz aus, den Sie sich gut merken können, z. B. „Diese Praxistipps sichern mein WLAN“.

Nun nehmen Sie jeweils die Anfangsbuchstaben und setzen einige Sonderzeichen dazwischen: „D-P*s-m_W*“. Und schon haben Sie ein sicheres Passwort. Alternativ nutzen Sie einen kostenlosen Passwort Manager.

Tipp: Sollten Sie Ihren Netzwerkschlüssel vergessen oder verlieren, können Sie das Gerät auf den Auslieferungszustand zurücksetzen. Lesen Sie im Handbuch Ihres Routers nach, wie Sie dazu vorgehen müssen. Nach dem Zurücksetzen gilt wieder der bereits erwähnte Netzwerkschlüssel auf der Unterseite des Gerätes.



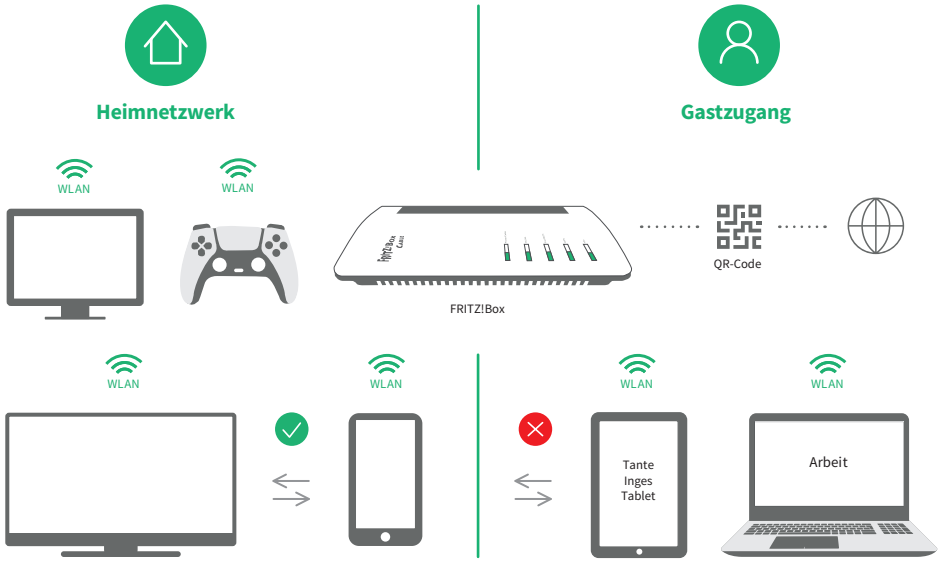
4. Verschlüsselung

Damit der Datenverkehr zwischen dem WLAN-Router und den Endgeräten nicht direkt abgehört werden kann, wird er verschlüsselt. Der aktuelle Standard ist WPA2. Er ist aber nur die zweitbeste Lösung, da mittlerweile diese Verschlüsselung auch mit etwas Geduld geknackt werden kann. Der neueste Standard ist WPA3. Dieser wird jedoch nicht von allen Endgeräten unterstützt. Deshalb empfiehlt sich die Einstellung **WPA2/WPA3**: Wenn ein Endgerät WPA3 unterstützt, verwendet der Router WPA3, ansonsten WPA2.

Zugang zum Netzwerk beschränken

1. Gastzugang

Für Gäste, die Ihr WLAN nutzen möchten, sollten Sie ein Gastnetzwerk einrichten. Dieses ist vom restlichen WLAN getrennt. Auf diese Weise kann ein Gast nicht auf Ihr Heimnetzwerk zugreifen und somit weder Informationen erhalten, die nicht für ihn bestimmt sind, noch Schaden anrichten.



Der Gastzugang besteht aus einer **eigenen SSID** (Netzwerkname) und einem **eigenen WLAN-Netzwerkschlüssel**. Die Zugangsdaten können Sie Ihren Gästen auch über einen QR-Code zur Verfügung stellen.

Bei der FRITZ!Box gibt es neben dem hier beschriebenen Gastzugang noch eine zweite Variante: den **öffentlichen WLAN-Hotspot**. Dieser besteht nur aus einer SSID, ist aber unverschlüsselt und benötigt daher auch keinen WLAN-Netzwerkschlüssel.

2. Zugangsprofile

Sie können für einzelne WLAN-Benutzer festlegen, zu welchen Zeiten und wie lange diese auf das Internet zugreifen dürfen. Außerdem können Sie bestimmte Internetadressen sperren.

Dazu rufen Sie „Heimnetz > Zugangsprofile“ auf. Dort finden Sie drei ab Werk eingerichtete Zugangsprofile:

Standard: Automatisch zugewiesenes Zugangsprofil für Geräte, die sich zum ersten Mal einwählen. Dieses Profil können Sie ändern.

Gast: Dieses gilt für alle Geräte, die sich im Gastnetz anmelden. Es kann ebenfalls geändert werden.

Unbeschränkt: Uneingeschränkte Internetnutzung; nicht änderbar.

Sie können weitere, individuell definierte Zugangsprofile anlegen. Dies ist besonders praktisch, um die Internetnutzung von Kindern zu kontrollieren:

Zugänglichkeit: An welchen Wochentagen und zu welchen Tages- bzw. Nachtzeiten ist das Internet für sie zugänglich bzw. nicht zugänglich?

Zeitbudget: An welchen Wochentagen und zu welchen Tages-/Nachtzeiten dürfen sie wie viel Zeit im Internet verbringen? Hier können Sie auch verhindern, dass ein Kind dieses „Zeitbudget“ umgeht, indem es sich von mehreren Geräten aus einwählt.

Adressfilter: Hierbei handelt es sich um Internet-Adressen, die für das Kind gesperrt sind. Dazu gibt es den Button „Jugendgefährdende Inhalte sperren (BPjM-Modul)“: Damit werden mit einem Klick alle Adressen gesperrt, die in der Liste der BPjM (Bundeszentrale für Kinder- und Jugendmedienschutz) als kritisch aufgeführt sind.

Zugangsprofile weisen Sie einem Nutzer unter „Heimnetz“ -> „Netzwerk“ zu.

Tipp: Aktivieren Sie bei Zugangsprofilen, die die Internetnutzung einschränken sollen, immer die Option „Nutzung des Gastzugangs gesperrt“. Damit verhindern Sie, dass sich ein Benutzer einfach als Gast einloggt, um die Einschränkungen zu umgehen.

Die Option „Portfreigabe automatisch“ sollten Sie aus Sicherheitsgründen nicht verwenden.

Wichtig: Überprüfen Sie von Zeit zu Zeit, welche Portfreigaben noch benötigt werden und gelöscht werden können. Weitere Informationen dazu finden Sie im Bereich „Portfreigaben“.

3. MAC-Adressfilter

Jedes Gerät hat eine eindeutige MAC-Adresse (MAC = Media Access Control). Bei der FRITZ!Box können Sie festlegen, dass sich nur bestimmte Endgeräte mit dem Router verbinden dürfen. Navigieren Sie dazu zu „WLAN > Sicherheit“ und aktivieren Sie im Abschnitt „WLAN-Zugriff beschränken“ die Option „WLAN-Zugriff auf bekannte WLAN-Geräte beschränken“. Nun können nur noch die hier aufgeführten Geräte das WLAN nutzen.

Wenn Sie neue Geräte in die Liste aufnehmen möchten, können Sie den MAC-Adressfilter vorübergehend deaktivieren, damit das Gerät automatisch in die Liste aufgenommen wird - oder Sie tragen die MAC-Adresse manuell ein.

Achtung: Ein MAC-Adressfilter allein reicht nicht aus, um unerwünschte Zugriffe zu verhindern. Da MAC-Adressen im WLAN unverschlüsselt übertragen werden und leicht verändert werden können (“MAC-Spoofing”), reichen sie nicht aus, um WLAN-Geräte sicher zu identifizieren. Dies gilt insbesondere für moderne Mobilgeräte, die für WLAN-Verbindungen täglich eine neue, zufällig generierte MAC-Adresse verwenden.

Weitere Maßnahmen

1. Portfreigaben

Ein Internet-Port ist eine Nummer, die Routern und Computern mitteilt, welche Anwendung ein Datenpaket verarbeiten soll. Einfach ausgedrückt ist es eine Tür, durch die ein Datenpaket gehen soll.

Da es sehr viele Port-Nummern gibt, besteht immer die Gefahr, dass sich ein Hacker einen Port aussucht, der sich zum Einschleusen von Schadsoftware eignet.

Deshalb sorgen Firewall-Anwendungen dafür, dass nur die wirklich benötigten Ports zugänglich sind. Bildlich gesprochen werden nur die notwendigen Türen offengehalten und alle anderen geschlossen.

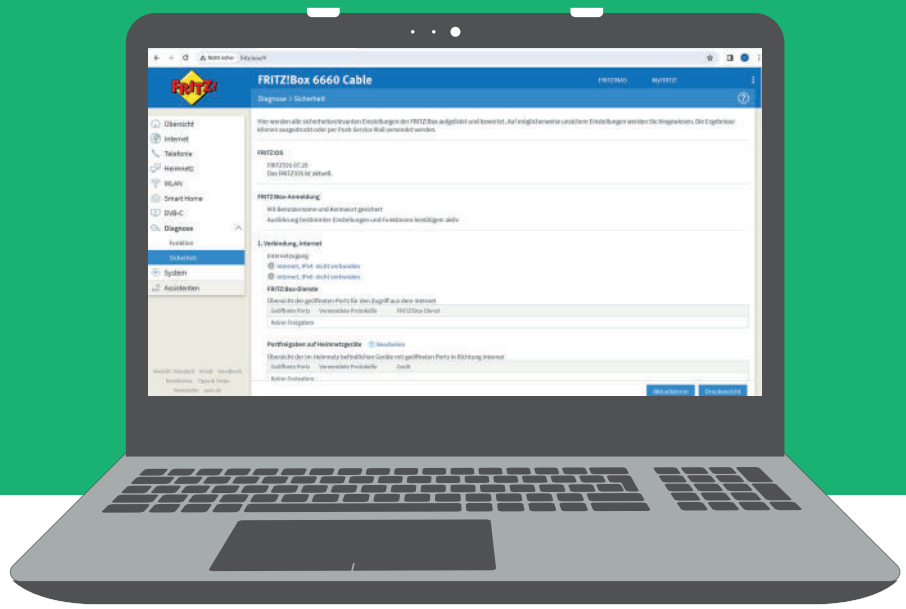
Nun kann es aber vorkommen, dass ein Gerät oder eine Anwendung einen Port benötigt, der von der Firewall geschlossen ist. In diesem Fall können Sie einen Port manuell öffnen, indem Sie „Internet > Freigaben > Portfreigaben“ aufrufen und dort „Gerät zur Freigabe hinzufügen“ auswählen.

2. Updates

Die Software des Routers wird ständig verbessert, insbesondere im Hinblick auf Schwachstellen, die von Hackern ausgenutzt werden könnten.

Tipp: Bei Geräten, die Sie über SYNVIA mieten, müssen Sie sich nicht um Updates kümmern – dies wird automatisch für Sie erledigt.

Bei der FRITZ!Box können Sie Updates automatisch einspielen lassen. Navigieren Sie dazu zu „System > Update > Auto-Update“ und aktivieren Sie dort die Option „Über neue FRITZ!OS-Versionen informieren und neue Versionen automatisch installieren“. Alternativ können Sie das Update auch manuell durchführen. Dazu laden Sie das Update von der Download-Seite von AVM herunter und folgen den Anweisungen im Menü „System > Update“.



3. Sicherheitsdiagnose

Die FRITZ!Box bietet eine komfortable Übersicht über die verschiedenen Sicherheitseinstellungen. Rufen Sie dazu den Menüpunkt „Diagnose > Sicherheit“ auf.

Dort können Sie folgende Informationen überprüfen:

- OS: Ist die Firmware noch aktuell oder ist ein Update notwendig?
- Anmeldung: Ist der Zugang zur Benutzeroberfläche ausreichend gesichert?
- Internetverbindung: Sind die richtigen Ports geöffnet oder geschlossen? Welche Filter sind für den Internetzugang eingerichtet?
- MyFRITZ! Kann von außen auf die Benutzeroberfläche des Routers zugegriffen werden und ist dieser Zugriff ausreichend gesichert?
- Ausgehende Filter: Welche Filter sind aktiv?

Sichern Sie auch Ihre Endgeräte ab

Um sich vor Cyberkriminalität zu schützen, sollten Sie neben Ihrem Netzwerk auch Ihre Endgeräte absichern. Hier die wichtigsten Tipps dazu:

- ✓ Verwenden Sie im Alltag ein normales Benutzerkonto, nicht das Standardkonto Administrator. Damit verhindern Sie, dass ein Hacker die Systemeinstellungen verändern kann.
- ✓ Achten Sie darauf, dass keine Verzeichnisse oder Dateien im Netzwerk freigegeben sind. Falls Sie dies ausnahmsweise trotzdem tun müssen, behalten Sie diese Freigaben im Auge und deaktivieren sie so bald wie möglich.
- ✓ Benutzen Sie eine Festplattenverschlüsselung. Damit bewirken Sie, dass Hacker mit den bei Ihnen vorgefundenen Daten nichts anfangen können. Windows bietet (je nach Version) die kostenlose Verschlüsselung Bitlocker an.
- ✓ Aktivieren Sie eine Software-Firewall auf Ihrem Gerät.
- ✓ Installieren Sie eine aktuelle Virenschutz-Software.

Tipp: Im G DATA Sicherheitspaket von SYNVIA sind Virenschutz und Firewall bereits integriert.

G DATA TRUST IN GERMAN SICHERHEIT

AV comparatives ADVANCED+ Malware Protection SEP 2020

AV TEST av-test.org CERTIFIED WINDOWS TOP PRODUCT

Notizen

Ratgeber WLAN-Guide

ZUM RATGEBER

Wenn Ihr privates WLAN langsam ist, nicht funktioniert oder sogar ganz ausfällt, dann ist dieser Ratgeber genau das Richtige für Sie. Hier erfahren Sie, wie Sie dem Problem auf die Spur kommen, welche Möglichkeiten Sie haben, es zu beheben und wie Sie Ihre WLAN-Verbindung generell optimieren können.

synvia.info/ratgeber-wlan-guide

Ratgeber WLAN optimal konfigurieren

ZUM RATGEBER

Erfahren Sie, wie Sie Ihr WLAN optimal konfigurieren, damit Ihr Netzwerk überall im Gebäude gut erreichbar ist und die bestmögliche Leistung liefert.

synvia.info/ratgeber-wlan-konfigurieren

Sie haben Fragen?
Wir haben Antworten.

www.synvia.de/service

In unserem Service-Bereich finden Sie weitere Ratgeber, unser Magazin, die Schnelle Hilfe mit Videoanleitungen und Antworten auf die häufigsten Fragen.

Schauen Sie gerne vorbei!

SYNVIA ist ein sehr guter Service besonders wichtig. Daher erreichen Sie uns schnell und unkompliziert unter der SYNVIA Kundenhotline.

Probieren Sie es aus! Wir beraten Sie gern.

kundenservice@synvia.de

0800 40 33 333

Mo – Fr: 08.00 – 20.00 Uhr, Sa: 08.00 - 16.30 Uhr

aus allen deutschen Netzen kostenfrei

www.synvia.de

Änderungen/Irrtümer vorbehalten. Stand 06.2025 – Alle Preise inkl. MwSt.