

MEINE DATEN!

Die besten Tipps gegen Datendiebstahl und Hackerangriffe

- E-Mails, Dateien und Benutzerkonten absichern
- Virenschutz, Spam-Abwehr, Surfen ohne Datenspuren
- Onlinebanking und -shopping ohne Risiko
- Daten verschlüsseln, sichern, wiederherstellen



Darauf sollten Sie bei der Internetverbindung achten



Online einkaufen, mit Freunden chatten oder schnell mal bei Google prüfen, wo in der Nähe ein gutes Restaurant ist: Für viele ist das Internet mittlerweile zu einer Selbstverständlichkeit geworden. Die Nutzung beschränkt sich schon lange nicht mehr nur auf den heimischen PC oder den Computer im Büro. Auch unterwegs gehen wir mit Smartphone, Tablet und Notebook online. Besteht die Internetverbindung erst einmal, machen sich viele Anwender keinerlei Gedanken mehr darüber, ob diese auch sicher ist. Doch leider gibt es zahlreiche Schlupflöcher, über die Cyberkriminelle Zugriff auf Ihre Geräte erhalten. Das reicht von fehlenden Passwörtern, mit denen Router und WLAN gesichert sein sollten, bis hin zur unverschlüsselten Datenübertragung. Bereits mit wenigen, leicht umsetzbaren Tricks können Sie potenziellen Angreifern den Zugriff auf Ihre Geräte über das Internet schwer machen.

Sicherheitseinstellungen für den Router

Das Drehkreuz zwischen dem Internet und den heimischen Geräten – sei es ein PC, Tablet, Smartphone, Drucker oder Ähnliches – ist der Router. Vereinfacht gesagt ist der Router für die Verteilung von Datenpaketen im Netzwerk zuständig. So sorgt er z. B. dafür, dass die aus dem Internet ankommenden Datenpakete korrekt an die einzelnen Geräte weitergeleitet werden oder auch die innerhalb des Heimnetzwerks verschickten Datenpa-



FRITZ!Box 5491 (Foto: AVM)

kete (etwa vom PC zum Netzwerkdrucker) ihr Ziel erreichen. Zu den bekanntesten Routern zählen die FRITZ!Box-Modelle von AVM sowie der Speedport-Router der Telekom. Bei den meisten Routern handelt es sich heutzutage um WLAN-Router, die neben der kabelgebundenen Datenübertragung auch die kabellose Übertragung via Funksignal ermöglichen.

Tipp
019

Die Internetverbindung steht – warum mehr tun?

Router werden von den Herstellern mittlerweile so ausgeliefert, dass sie sich bequem einrichten lassen und somit bereits nach kurzer Zeit die Verbindung ins Internet genutzt werden kann. Viele Anwender belassen es bei den Werkseinstellungen, die in puncto Sicherheit allerdings doch etwas zu wünschen übrig lassen. Entdecken Cyberkriminelle eine der Sicherheitslücken, gelingt ihnen damit nicht nur der Zugriff auf den Router selbst, sondern auch auf alle angeschlossenen Geräte. Ein Beispiel hierzu: Vor einigen Jahren wurde ein spektakulärer Angriff auf die FRITZ!Box von AVM bekannt, in der ein von außen steuerbares Telefoniegerät in der FRITZ!Box eingerichtet wurde, über das zahlreiche kurze Anrufe auf teure Auslandsnummern und ausländische Mehrwertnummern getätigt wurden. Die Geschädigten wurden erst durch die extrem hohe Telefonrechnung auf den Angriff aufmerksam. Manche Angriffe bleiben vom Anwender aber auch vollkommen unbemerkt, etwa wenn der eigene PC plötzlich Teil eines sog. *Botnetzes* wird (siehe dazu den folgenden Kasten »Gefahr durch unerkannte Botnetze«).

Gefahr durch unerkannte Botnetze

Vielleicht haben Sie auch schon einmal den Begriff *Botnetz* (engl. *Botnet*) gehört. Hierbei werden Tausende von Compu-

tern, die mit einem speziellen Schadprogramm infiziert wurden, zu einem Netzwerk zusammengeschlossen. Ein Computer innerhalb eines solchen Botnetzes wird als *Bot* bezeichnet. Da der Computer vom Botnetz-Betreiber ferngesteuert wird, ist häufig auch von einem *Zombie-PC* die Rede. Das Botnetz nutzt die Rechenleistung und Daten des infizierten Computers, ohne dass dessen Besitzer davon weiß, geschweige denn je seine Einwilligung erteilt hat. Ist ein Computer erst mal Teil eines Botnetzes, wird er häufig für illegale Zwecke, wie etwa das Versenden von Spam-Mails, eingesetzt. Es gibt mittlerweile aber auch legale Einsatzbereiche, etwa zu Forschungszwecken. Dass Ihr Computer Teil eines Botnetzes ist, lässt sich höchstens durch eine langsamere Internetverbindung und deutlich schwächere Rechenleistung feststellen. Meist bleibt die Infektion aber unentdeckt. Schutz vor einem Botnetz bieten eine Vielzahl der im Buch aufgeführten Tipps, wie etwa der Einsatz einer Sicherheitssoftware oder auch die Aktualisierung jeglicher Software inklusive der *Firmware* des Routers, wie z. B. in Tipp 021 auf Seite 53 gezeigt.

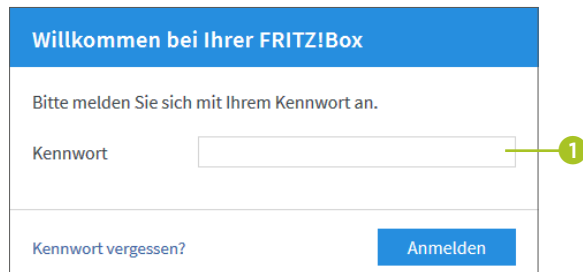
Passwort des Routers ändern

Tipp
020

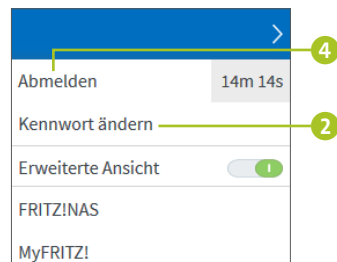
Wenn Sie die Einstellungen der FRITZ!Box ändern möchten, starten Sie den Browser (z.B. Firefox, Safari oder Google Chrome) und rufen die Adresse <http://fritz.box> auf. Beim Speedport-Router lautet die Adresse <http://speedport.ip>. Bevor Sie die Benutzeroberfläche des Routers zu Gesicht bekommen, wird ein Passwort abgefragt. Bei vielen Geräten wird dieses Router-Passwort bereits ab Werk voreingestellt. Das Passwort können Sie je nach Gerät entweder auf der Unterseite des Routers ablesen oder auch über die Support-Webseiten des Herstellers ausfindig machen. Wer herausfindet, welches Modell von welchem Anbieter Sie im Einsatz haben, hat leichten Zugang zu Ihrem Router (lesen Sie hierzu auch

Tipps. Wenn Sie einen Passwort-Manager wie LastPass einsetzen, können Sie auch den Passwort-Generator für die Erzeugung des Passwortes nutzen (siehe den Kasten »Sichere Passwörter mithilfe des Passwort-Generators erzeugen« auf Seite 29). Bestätigen Sie das Passwort mit **Übernehmen**.

1. Starten Sie den Browser, und rufen Sie die Adresse `http://fritz.box` auf. Melden Sie sich mit dem vom Hersteller vorgegebenen Kennwort an **1**. Sollten Sie das Passwort bereits zu einem früheren Zeitpunkt selbst geändert haben, sollten Sie es aus Sicherheitsgründen trotzdem regelmäßig austauschen.

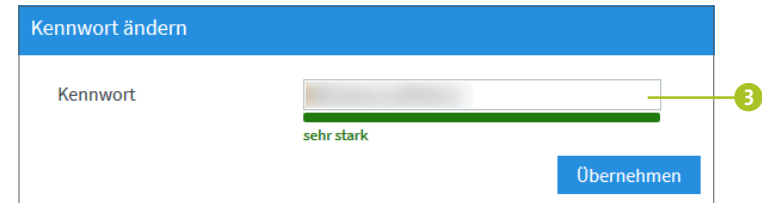


2. Befinden Sie sich in der Benutzeroberfläche der FRITZ!Box, klicken Sie oben rechts auf das kleine Symbol mit den drei Punkten **3**. Im aufklappenden Menü wählen Sie den Befehl **Kennwort ändern** **2**.



3. Geben Sie im Feld **Kennwort** ein neues Passwort ein **3**. Der Balken unterhalb des Feldes zeigt, wie »stark«, d.h. wie gut das Passwort ist. Berücksichtigen Sie bei der Passwortwahl die im vorherigen Kapitel vorgestellten

Tipps. Wenn Sie einen Passwort-Manager wie LastPass einsetzen, können Sie auch den Passwort-Generator für die Erzeugung des Passwortes nutzen (siehe den Kasten »Sichere Passwörter mithilfe des Passwort-Generators erzeugen« auf Seite 29). Bestätigen Sie das Passwort mit **Übernehmen**.

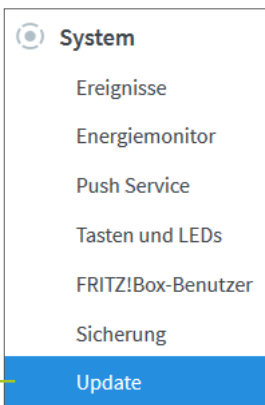


Wenn Sie gleich im Anschluss auch die folgenden Tipps ausprobieren möchten, bleiben Sie bei der FRITZ!Box-Oberfläche angemeldet. Wenn Sie die Konfiguration des Routers unterbrechen müssen, sollten Sie sich unbedingt abmelden. Hierzu reicht ein Klick auf das Symbol mit den drei Punkten und dann auf **Abmelden** **4**. Für die folgenden Tipps müssen Sie sich dann natürlich wieder anmelden, wie in Schritt 1 gezeigt – nun allerdings mit Ihrem selbst erstellten Passwort.

Firmware-Update installieren

Tipps
021

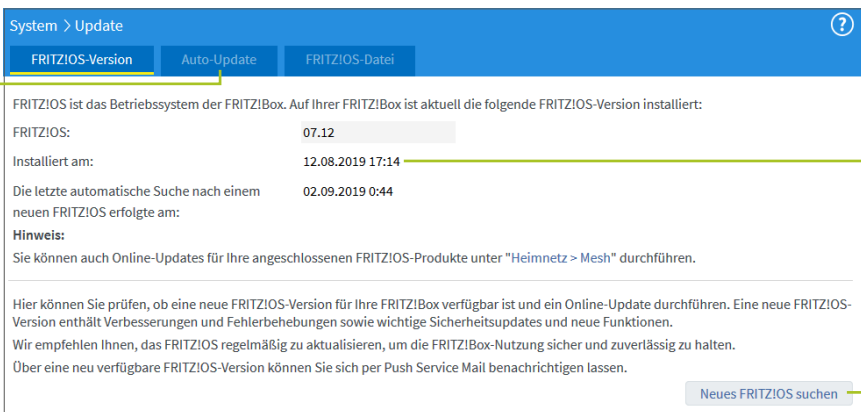
Die Hersteller von Routern veröffentlichen regelmäßig aktualisierte Versionen der Firmware (sprich des Betriebssystems des Routers). Diese enthalten nicht nur neue Funktionen, sondern auch Fehlerbehebungen. Aus Sicherheitsgründen sollten Sie immer die neueste Firmware installieren. Für das Betriebssystem der FRITZ!Box, *FRITZ!OS* genannt, geschieht dies im Normalfall automatisch. Um die Einstellungen sicherheitshalber zu überprüfen, gehen Sie folgendermaßen vor:



1. Stellen Sie nach der Anmeldung in der Benutzeroberfläche zunächst sicher, dass die erweiterte Ansicht aktiviert ist. Hierzu klicken Sie auf das Symbol . Der Regler rechts von **Erweiterte Ansicht** sollte grün gefärbt sein.

2. Klicken Sie in der Benutzeroberfläche der FRITZ!Box links auf **System** ► **Update** ①.

3. Rechts erfahren Sie im Register **FRITZ!OS-Version**, wann die letzte Version des Betriebssystems installiert wurde ②. Liegt die Installation bereits geraume Zeit zurück, sollten Sie über die Schaltfläche **Neues FRITZ!OS suchen** ③ die Suche nach einer neuen Version starten und diese anschließend installieren.



4. Die Einstellungen zur automatischen Installation wichtiger Updates überprüfen Sie im Register **Auto-Update** ④. Hier sollte mindestens **Stufe II** ausgewählt sein ⑤. In diesem Fall werden Sie über neue FRITZ!OS-Versionen informiert. Die notwendigen Updates werden außerdem

automatisch durchgeführt. Sollten Sie hier Änderungen an den Einstellungen vorgenommen haben, müssen Sie diese mit **Übernehmen** bestätigen.

5 Stufe II: Über neue FRITZ!OS-Versionen informieren und notwendige Updates automatisch installieren (Empfohlen)

Weitere FRITZ!Box-Geräte aktualisieren

Haben Sie von AVM noch weitere Geräte im Einsatz, wie etwa einen Repeater, um die Reichweite des WLANs zu erhöhen, oder einen Powerline-Adapter, um Ihre Computer über das interne Stromnetz der Wohnung zu vernetzen? Auch diese Geräte sollten immer auf dem neuesten Stand sein. Um dies zu überprüfen, rufen Sie in der Benutzeroberfläche der FRITZ!Box links **Heimnetz** ► **Mesh** auf. Blättern Sie rechts in der **Mesh-Übersicht** nach unten bis zur Auflistung der Heimnetzgeräte. Überprüfen Sie in der Spalte **Update**, ob für eines der Geräte eine Aktualisierung vorliegt. Mit einem Klick auf **Update ausführen** stoßen Sie dieses an.

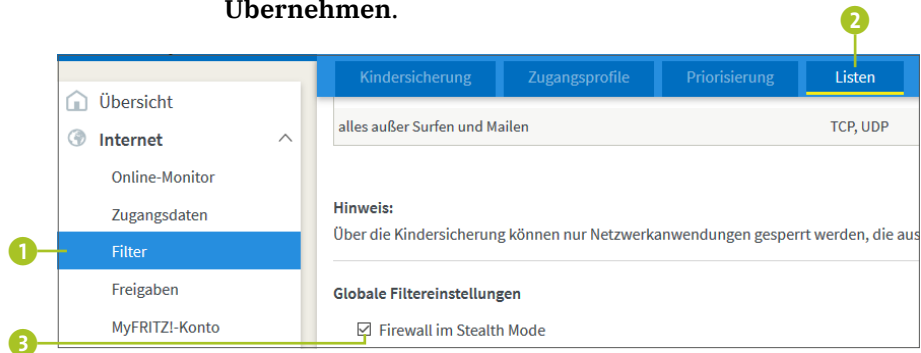
Router-Firewall im Stealth-Modus betreiben

Tipp
022

Die meisten Router haben mittlerweile eine Firewall an Bord, deren Aufgabe es ist, den ein- und ausgehenden Datenverkehr zu überprüfen und unerwünschte Datenpakete abzublocken. Dies gilt auch für die FRITZ!Box. Sogenannte *Ping*-Anfragen, mit denen Angreifer zunächst nur das Vorhandensein der IP-Adresse prüfen, werden in den Standardeinstellungen allerdings nicht verhindert. Fällt eine solche Ping-Anfrage positiv aus, erhält der Angreifer die Bestätigung, dass die IP-Adresse vergeben ist. Damit rentiert sich für ihn ein richtiger Angriff. Eine wichtige Sicherheitseinstellung besteht also darin, derartige Anfragen zu verhindern. Hierzu muss die

Firewall im sog. *Stealth-Modus* betrieben werden. Um ihn zu aktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der linken Spalte der Benutzeroberfläche der FRITZ!Box auf **Internet ▶ Filter** ①.
2. Wechseln Sie in der rechten Fensterhälfte in das Register **Listen** ②. Blättern Sie nun ganz nach unten bis zum Bereich **Globale Filtereinstellungen**.
3. Versetzen Sie das Kästchen vor **Firewall im Stealth Mode** mit einem Häkchen ③. Bestätigen Sie die Einstellung mit **Übernehmen**.



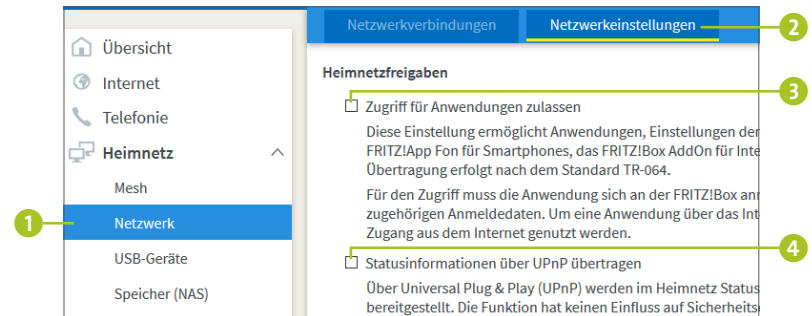
Tipp 023

Berechtigungen für Portfreigabe unterbinden

Ob Fitnessuhr oder das Smart-TV-Gerät: Beide zählen zum *Internet der Dinge* (kurz: IoT für *Internet of Things*). Diese IoT-Geräte werden meist per WLAN an das Heimnetzwerk angeschlossen. Hierfür nutzen die Geräte *UPnP* (Abkürzung für *Universal Plug and Play*), das eine Kommunikation zwischen Geräten unterschiedlicher Hersteller ermöglicht. Ist in Ihrem Router UPnP aktiviert, kann allerdings jedes beliebige Gerät und auch jede Software inklusive Schadprogramme im Heimnetzwerk den Router konfigurieren und so z. B. bestimmte Ports in der Firewall öffnen (lesen Sie hierzu auch den Kasten »Vorsicht mit der Freigabe von Ports« auf Sei-

te 95). Aus Sicherheitsgründen sollten Sie UPnP deshalb in Ihrem Router deaktivieren. In der FRITZ!Box gehen Sie hierzu folgendermaßen vor:

1. Rufen Sie in der Benutzeroberfläche der FRITZ!Box links nacheinander **Heimnetz ▶ Netzwerk** ① auf. Wechseln Sie dann rechts in das Register **Netzwerkeinstellungen** ②.
2. Blättern Sie auf der Seite nach unten bis zu den **Heimnetzfreigaben**. Hier entfernen Sie das Häkchen vor **Zugriff für Anwendungen zulassen** ③. Die **Statusinformationen über UPnP übertragen** ④ können Sie wiederum aktiviert lassen. Bestätigen Sie mit **Übernehmen**.



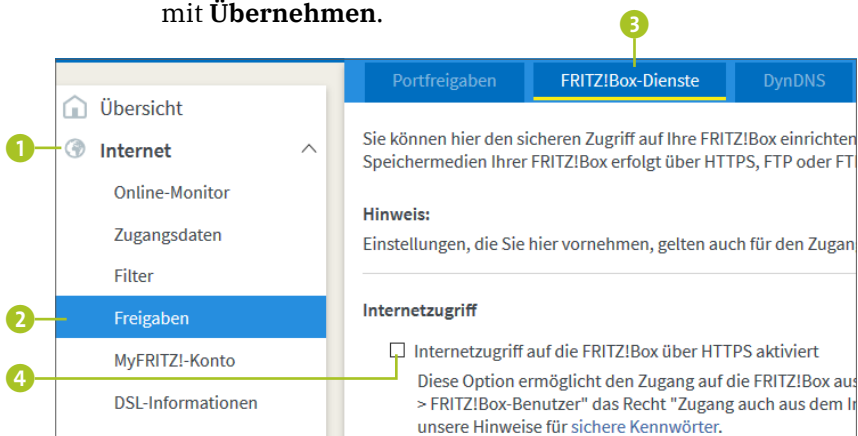
Portfreigaben für ein bestimmtes Gerät erteilen

Eine Spielekonsole, die Sie gerne nutzen, benötigt unbedingt UPnP, um die Portfreigaben des Routers steuern zu können? In der FRITZ!Box ist es möglich, nur ganz bestimmten Geräten die Portfreigabe zu erlauben. Rufen Sie hierzu **Heimnetz ▶ Netzwerk** auf, und markieren Sie rechts das Register **Netzwerkverbindungen**. Suchen Sie in der folgenden Liste das gewünschte Gerät, und klicken Sie auf das Stiftsymbol rechts, um die Einstellungen für dieses Gerät zu öffnen. Auf der folgenden Seite aktivieren Sie **Selbstständige Portfreigaben für dieses Gerät erlauben** und bestätigen mit **OK**.

Fernzugriff nur dann, wenn nötig

Auf die Benutzeroberfläche der FRITZ!Box lässt sich auch von unterwegs aus zugreifen. Der entsprechende Dienst nennt sich *MyFRITZ!*. Um ihn nutzen zu können, müssen Sie sich einmal in der Benutzeroberfläche der FRITZ!Box über **Internet ▶ MyFRITZ!-Konto** mit einer E-Mail-Adresse registrieren. Anschließend können Sie z. B. über die MyFRITZ!-App von Ihrem Smartphone aus auf eine an die FRITZ!Box angeschlossene USB-Festplatte zugreifen. Was Ihnen möglich ist, kann aber auch Angreifern gelingen. Wer diesen Dienst also nicht wirklich dringend benötigt, sollte aus Sicherheitsgründen lieber darauf verzichten. Um sicherzustellen, dass der Fernzugriff deaktiviert ist, gehen Sie folgendermaßen vor:

1. Klicken Sie in der linken Spalte der Benutzeroberfläche der FRITZ!Box auf **Internet** **1** und dann auf **Freigaben** **2**.
2. Rufen Sie rechts das Register **FRITZ!Box-Dienste** **3** auf.
3. Stellen Sie sicher, dass das Kästchen vor **Internetzugriff auf die FRITZ!Box über HTTPS aktiviert** nicht mit einem Häkchen versehen ist **4**. Sollte der Dienst aktiviert sein, entfernen Sie das Häkchen per Mausklick und bestätigen mit **Übernehmen**.




Das private WLAN schützen

Ein *WLAN* (Abkürzung für *Wireless Local Area Network*) in den eigenen vier Wänden ist ausgesprochen praktisch. Nur wenige Schritte sind nötig, und schon sind Computer, Tablet, Smartphone und mehr mit dem Internet und dem Heimnetzwerk verbunden – und das ganz ohne Kabelsalat. Wie für den Router gilt auch für das Funknetzwerk: Übernehmen Sie nicht blind die Werkseinstellungen des Herstellers, sondern überprüfen Sie die Sicherheitseinstellungen, um Ihr privates WLAN vor Angriffen von außen zu schützen. Sie stellen damit zugleich sicher, dass keine Person außerhalb Ihrer eigenen vier Wände über Ihr WLAN eine Verbindung ins Internet herstellt. Denn denken Sie daran: Sie haften für alles (legal oder illegal), was über Ihre Internetverbindung geschieht.

Eigenen Namen für WLAN vergeben

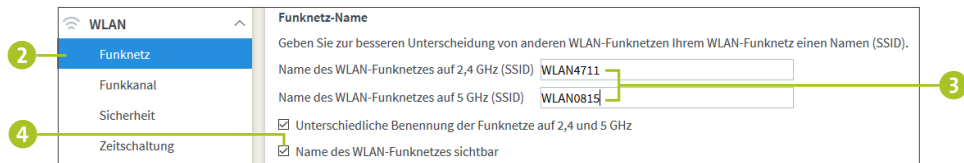
Jedes Funknetzwerk verfügt über einen Namen, die sog. *SSID* (Abkürzung für *Service Set Identifier*). Dies gilt natürlich auch für Ihr eigenes, privates WLAN daheim. Per Werkseinstellung vergeben Hersteller wie AVM hier meist den Namen des Routers, also z. B. *FRITZ!Box 4790*. Diese Angabe lässt nicht selten aber auch Rückschlüsse auf das per Werk vergebene Passwort zu (siehe hierzu auch den nächsten Tipp). Doch die SSID des WLANs ist schnell geändert:

1. Melden Sie sich in der Benutzeroberfläche der FRITZ!Box an, so wie in Tipp 020 auf Seite 51 gezeigt. Stellen Sie nach einem Klick auf das Symbol  sicher, dass **Erweiterte Ansicht** aktiviert ist **1**.

Erweiterte Ansicht



2. Klicken Sie in der linken Spalte auf **WLAN** und dann auf **Funknetz** 2. Blättern Sie in der rechten Fensterhälfte nach unten bis zum Bereich **Funknetz-Name**.
3. Die meisten Modelle der FRITZ!Box arbeiten sowohl mit dem 2,4-GHz-Frequenzband als auch mit dem 5-GHz-Frequenzband. Vergeben Sie für jedes einen eigenen Namen 3. Dieser sollte weder einen Rückschluss auf den verwendeten Router zulassen, noch auf Sie oder Ihr Haus hinweisen. Name, Straße und Hausnummer sind also keine gute Wahl. Damit es keine Probleme mit Funknetzen in der Nachbarschaft gibt, sollten Sie einen noch nicht vergebenen Namen wählen.



4. Bestätigen Sie die Eingaben mit **Übernehmen**.

Funknetz-Namen unsichtbar machen

Immer wieder hört man den Rat, den Namen des WLANs zu verbergen, frei nach dem Motto: »Was man nicht sieht, kann man auch nicht finden«. Umgesetzt ist dieser Ratschlag schnell: Einfach unter **WLAN** ► **Funknetz** im Bereich **Funknetz-Name** das Häkchen vor **Name des WLAN-Funknetzes sichtbar** 4 entfernen, mit **Übernehmen** bestätigen, und schon erscheint das WLAN nicht mehr in der Liste der verfügbaren Funknetzwerke. Die bereits angemeldeten Geräte bleiben dabei weiterhin mit dem WLAN verbunden. Um vor den Nachbarn das WLAN zu verbergen, mag der Tipp geeignet sein. Einen Profi, der über ein Spähprogramm verfügt, hält eine versteckte SSID allerdings nicht ab!

Am Passwort führt kein Weg vorbei

Tipps für die Wahl eines sicheren Kennwortes	13
TIPP 001 Warum simple Buchstaben- oder Ziffernfolgen keine gute Wahl sind	14
TIPP 002 Das richtige Passwort finden	15
TIPP 003 Jedes Konto verdient sein eigenes Passwort	17
TIPP 004 Passwörter regelmäßig ändern	17
Der Passwort-Manager als Gedächtnisstütze	18
TIPP 005 Die Vorteile eines Passwort-Managers	19
TIPP 006 Cloubasiert oder lokal	19
TIPP 007 Allgemeine Informationen zum Passwort-Manager LastPass	20
TIPP 008 Den Passwort-Manager LastPass installieren	21
TIPP 009 Bei LastPass anmelden	25
TIPP 010 Auf einer Webseite eingetragene Zugangsdaten in LastPass speichern	28
TIPP 011 Zugangsdaten direkt im Passwort-Tresor von LastPass eintragen	30
TIPP 012 Bei einem Online-Dienst mithilfe von LastPass anmelden	32
TIPP 013 Sicherheitseinstellungen ändern und bei LastPass abmelden	35
Doppelt hält besser: Die Zwei-Faktor-Authentisierung	37
TIPP 014 Das Grundprinzip der Zwei-Faktor-Authentisierung	38
TIPP 015 Einsatz der Zwei-Faktor-Authentisierung am Beispiel von LastPass	40
TIPP 016 Authentisierungs-App auf dem Smartphone installieren	42
TIPP 017 LastPass-Konto im Google Authenticator hinzufügen	43
TIPP 018 Mithilfe der 2FA bei LastPass anmelden	46

Darauf sollten Sie bei der Internetverbindung achten

Sicherheitseinstellungen für den Router	49
TIPP 019 Die Internetverbindung steht – warum mehr tun?	50
TIPP 020 Passwort des Routers ändern	51
TIPP 021 Firmware-Update installieren	53
TIPP 022 Router-Firewall im Stealth-Modus betreiben	55
TIPP 023 Berechtigungen für Portfreigabe unterbinden	56
TIPP 024 Fernzugriff nur dann, wenn nötig	58
Das private WLAN schützen	59
TIPP 025 Eigenen Namen für WLAN vergeben	59
TIPP 026 Verschlüsselungsmethode wählen und Passwort ändern	61
TIPP 027 Fremden Geräten den Zugriff auf das WLAN verwehren	62
TIPP 028 Gastzugang für Freunde einrichten	64
TIPP 029 WLAN auch mal deaktivieren	65
Tipps für die Internetverbindung unterwegs	67
TIPP 030 Wie sicher ist der Hotspot?	68
TIPP 031 Automatische Anmeldung an Hotspots unter Windows 10 deaktivieren	68
TIPP 032 Automatische Anmeldung unter Android deaktivieren	70
TIPP 033 Automatische Anmeldung auf dem iPhone deaktivieren	71
TIPP 034 Keine persönlichen, vertraulichen Daten übermitteln	72
Für mehr Sicherheit ein VPN nutzen	72
TIPP 035 ProtonVPN-App auf dem Smartphone installieren	73
TIPP 036 Bei der ProtonVPN-App anmelden	76
TIPP 037 VPN-Server auswählen und verbinden	76

So schützen Sie Ihren PC

Allgemeine Sicherheitseinstellungen für Ihren PC	79
TIPP 038 Benutzerrechte mithilfe des Standardkontos eingrenzen	80
TIPP 039 Betriebssystem auf dem neuesten Stand halten	83
TIPP 040 Programme und Apps immer aktualisieren	86
TIPP 041 Nicht benötigte Software entfernen	86
TIPP 042 Software und Treiber nur aus vertrauenswürdigen Quellen installieren	87
TIPP 043 Automatische Wiedergabe von Datenträgern deaktivieren	89
So schützt die Firewall vor Angriffen aus dem Netz	90
TIPP 044 Ein erster Blick: Ist die Firewall aktiviert?	91
TIPP 045 Übersicht über zugelassene Apps und Features	93
Die passende Sicherheitssoftware für Ihren PC	96
TIPP 046 Welche Sicherheitssoftware ist empfehlenswert?	96
TIPP 047 Führen Sie regelmäßig eine Überprüfung durch	99
Wichtige Datenschutzeinstellungen vornehmen	101
TIPP 048 Allgemeine Datenschutzeinstellungen anpassen	102
TIPP 049 App-Berechtigungen festlegen	105

Mit dem Smartphone sicher unterwegs

Sicherheitseinstellungen für das Smartphone	109
TIPP 050 Smartphone am besten per PIN oder Passwort sperren	109
TIPP 051 Kritischer Umgang mit Benachrichtigungen auf dem Sperrbildschirm	112
TIPP 052 Betriebssystem auf dem aktuellsten Stand halten	113
TIPP 053 Unterwegs das öffentliche WLAN nutzen?	113
TIPP 054 Antivirenprogramm – sinnvoll oder nicht?	114
Augen auf bei der Installation von Apps	116
TIPP 055 Apps nur aus vertrauenswürdigen Quellen installieren	116

TIPP 056 App-Berechtigungen auf einem Android-Smartphone	118
TIPP 057 App-Berechtigungen auf Android-Smartphone ändern	120
TIPP 058 Datenschutzeinstellungen auf dem iPhone prüfen	121
TIPP 059 Apps besser manuell aktualisieren	123

Kostenfallen auf der Spur	125
TIPP 060 Teure In-App-Käufe umgehen	125
TIPP 061 Gefälschte Apps erkennen	127
TIPP 062 Schutz vor Abo-Fallen	128

Für alle Fälle: Daten sichern

Backup-Maßnahmen für den PC einrichten	131
TIPP 063 Datensicherung unter Windows 10 aktivieren	132
TIPP 064 Gelöschte oder beschädigte Daten wiederherstellen	135
Daten sicher in der Cloud ablegen	137
TIPP 065 Vorsicht beim Anlegen des Benutzerkontos	138
TIPP 066 Sicherheitsrisiko Internetverbindung	138
TIPP 067 Zugriff auf die Cloud via Browser	139
TIPP 068 Ein sinnvoller zusätzlicher Schutz: Die Zwei-Faktor-Authentisierung	140
TIPP 069 Vor- und Nachteile einer Cloud-App	140
TIPP 070 Standort der Cloud-Server berücksichtigen	141
TIPP 071 Unverschlüsselte Datenspeicherung	141
TIPP 072 Cloud als beliebtes Ziel von Denial-of-Service-Attacken	142
TIPP 073 So sichern Sie Ihre iPhone-Daten in der iCloud	143
TIPP 074 Daten vom Android-Smartphone in Google Drive sichern	144

Zur Sicherheit: Daten verschlüsseln	146
TIPP 075 Boxcryptor auf einem Windows-PC installieren	146
TIPP 076 Bereits in OneDrive abgelegte Dateien und Ordner verschlüsseln	150
TIPP 077 Neuen verschlüsselten Ordner in OneDrive anlegen	152

Die Kommunikation per E-Mail absichern

Nur Werbung oder Phishing? Wie gefährlich ist die E-Mail? 155

TIPP 078 Wer ist wirklich der Absender der E-Mail? 156

TIPP 079 Wichtige Indizien: Betreff, Anrede, Formatierung, Stil und Sprache 156

TIPP 080 Methoden, um an sensible Daten zu gelangen 157

TIPP 081 Umgang mit in E-Mails enthaltenen Links 158

TIPP 082 Finger weg von Dateianhängen 159

TIPP 083 Was tun mit der verdächtigen E-Mail? 160

Wichtige Sicherheitseinstellungen für Outlook und Thunderbird ... 162

TIPP 084 E-Mails im HTML-Format versus Nur-Text-Format 163

TIPP 085 Automatisches Herunterladen von Bildern unterbinden 164

TIPP 086 E-Mail-Programm immer auf dem neuesten Stand halten 166

TIPP 087 Junk-E-Mail-Optionen in Outlook festlegen 167

TIPP 088 Unerwünschte Absender in Outlook blockieren 169

TIPP 089 Junk-Filter-Einstellungen in Thunderbird prüfen 170

TIPP 090 Unerwünschte Absender in Thunderbird blockieren 171

Wichtige Schutzmaßnahmen für den Browser

Sicher und ohne Spuren surfen 175

TIPP 091 Browser auf dem neuesten Stand halten 175

TIPP 092 Nutzungsdaten und Absturzberichte nicht weiterleiten 177

TIPP 093 Passwörter nicht vom Browser speichern lassen 179

TIPP 094 Der richtige Umgang mit Cookies 179

TIPP 095 Cookies, Krypto-Miner und Fingerprinter in Firefox blockieren 181

TIPP 096 Inkognito im Internet unterwegs 183

TIPP 097 Anonym im Internet mit dem Browser Opera und VPN 184

TIPP 098 Der richtige Umgang mit Add-ons und Plugins 185

TIPP 099 Sichere Einstellungen für Downloads und Pop-ups wählen 188

TIPP 100 Diskrete Suchmaschine einsetzen 190

Sichere Webseiten erkennen 191

TIPP 101 Nicht klicken, sondern prüfen und tippen 191

TIPP 102 Sichere, verschlüsselte Internetverbindung nutzen 193

TIPP 103 Phishing-Filter im Browser aktivieren 195

Gut geschützt: Bankgeschäfte im Internet erledigen

Darauf müssen Sie beim Online-Banking achten 199

TIPP 104 Diese Angriffe drohen beim Online-Banking 199

TIPP 105 Diese Sicherheitsmaßnahmen sollten Sie immer berücksichtigen 201

TIPP 106 Diese Verfahren zum Online-Banking stehen zur Auswahl 202

Sicherer Zahlungsverkehr im Internet 205

TIPP 107 Bezahlen per Rechnung, Nachnahme und Vorkasse 206

TIPP 108 SEPA-Lastschrift für den Einkauf nutzen 207

TIPP 109 Kreditkarte als Bezahlmethode wählen 207

TIPP 110 Eine Zahlung über Bezahlsysteme wie PayPal veranlassen 208

TIPP 111 Bezahlen per Sofortüberweisung 209

TIPP 112 Der neueste Trend: Mobiles Bezahlen mit dem Smartphone 210

Entspannt Reisen buchen und online shoppen

Ist der Anbieter vertrauenswürdig oder Fake? 213

TIPP 113 Preise vergleichen: Schnäppchen oder Wucher? 214

TIPP 114 Bewertungen sagen viel über Ware und Anbieter aus 215

TIPP 115 Zur Sicherheit die Webadresse überprüfen 217

TIPP 116 Gütesiegel und seine Gültigkeit überprüfen 218

TIPP 117 Wichtige Informationen rund um den Anbieter einholen 219

Wichtiges zur Registrierung und zum Kaufabschluss	222
TIPP 118 Verschlüsselte Internetverbindung ist ein Muss	222
TIPP 119 Passwortwahl und Zwei-Faktor-Authentisierung	223
TIPP 120 Wird die Button-Lösung gewährleistet?	224
Diese Rechte haben Sie als Käufer	225
TIPP 121 Der Fernabsatzvertrag regelt das Rückgaberecht	226
TIPP 122 Reiseveranstalter versus Reisevermittler: Wer ist haftbar?	226
TIPP 123 Für den Fall der Fälle alles dokumentieren	227

Schwachstellen in sozialen Netzwerken

Datensicherheit in sozialen Netzwerken	232
TIPP 124 Welche Informationen sollte man veröffentlichen, welche nicht?	232
TIPP 125 Einstellungen zur Privatsphäre prüfen	233
TIPP 126 Zugriff auf Kontaktdaten verbieten	235
TIPP 127 Vorsicht beim Veröffentlichen von Fotos und Videos	236
TIPP 128 Gesunde Skepsis bei Freundschaftsanfragen	236
TIPP 129 Achtung vor Fake-Profilen	237
Tipps für die Nutzung von Messengern	238
TIPP 130 WhatsApp im Fokus der Datenschützer	238
TIPP 131 Datenschutzeinstellungen von WhatsApp anpassen	239

Das richtige Troubleshooting

Wichtige Maßnahmen, falls Ihr Konto gehackt wurde	243
TIPP 132 Woran erkenne ich, dass mein E-Mail-Konto gehackt wurde?	244
TIPP 133 So prüfen Sie, ob Ihre E-Mail-Adresse bereits gehackt wurde	245
TIPP 134 Wichtige Schritte, wenn das E-Mail-Konto gehackt wurde	246
TIPP 135 Was tun, wenn mein Facebook-Konto oder Ähnliches gehackt wurde?	247

Verdacht auf Malware-Infektion ? So gehen Sie vor!	250
TIPP 136 Regelmäßig Scans durchführen	251
TIPP 137 Weitere Virencans im abgesicherten Modus durchführen	252
Im Fall der Fälle: PC zurücksetzen	256
TIPP 138 Einen älteren Computerzustand wiederherstellen	257
TIPP 139 Den Computer auf Werkseinstellungen zurücksetzen	259
Stichwortverzeichnis	263