

❖❖❖ WLAN ABSCHALTEN

Manche Router bieten die Möglichkeit, das WLAN zu bestimmten Uhrzeiten, z. B. nachts, abzuschalten.

Viele Router haben auch eine Taste oder einen Schalter, mit dem das WLAN manuell ein- und ausgeschaltet werden kann.



Schalten Sie Ihr WLAN ab, wenn Sie es nicht nutzen. Das spart Energie

❖❖❖ FIRMWARE ÜBERPRÜFEN

Die „Firmware“ ist die Betriebssoftware eines Routers.

Im Laufe der Zeit bringen Hersteller neuere Versionen der Firmware (Firmware-Updates) heraus, die z. B. den Router um Funktionen erweitert oder Sicherheitslücken schließt.

Daher sollte man in regelmäßigen Abständen die Aktualität der Firmware überprüfen und ggf. eine neuere Version der Firmware installieren. Eine aktuelle Firmware steht meist auf der Homepage des Herstellers zum Download bereit. Bei einigen Routern kann die Firmware aber auch direkt über die Benutzeroberfläche heruntergeladen und installiert werden.



Halten Sie die Firmware des Routers immer auf dem aktuellen Stand

❖❖❖ WLAN-REICHWEITE

Was tun bei schlechtem WLAN-Empfang innerhalb der Wohnung?

Grundsätzlich sollte der Router offen und möglichst hoch im Raum stehen, um eine optimale Reichweite zu erhalten. Steht der Router in einem Schrank bzw. zwischen Möbeln, so kann sich dies negativ auf die Reichweite auswirken. Ist die Reichweite trotzdem zu niedrig, so helfen WLAN-Repeater weiter. Ein Repeater sollte möglichst auf halber Strecke zwischen Router und dem am weitesten entfernten Gerät positioniert werden.

VOR ORT FÜR SIE DA!

Unsere Beratungsstellen Unsere Stützpunkte

67655 Kaiserslautern
Fackelstraße 22
Telefon: (0631) 92 881
kaiserslautern@vz-rlp.de

56068 Koblenz
Entenpfuhl 37
Telefon: (0261) 12 727
koblenz@vz-rlp.de

67059 Ludwigshafen
Wredestraße 33
Telefon: (0621) 51 21 45
ludwigshafen@vz-rlp.de

55116 Mainz
Seppel-Glückert-Passage 10
Telefon: (06131) 28 48 20
mainz@vz-rlp.de

66953 Pirmasens
Exerzierplatzstraße 1
Telefon: (06331) 12 160
pirmasens@vz-rlp.de

54290 Trier
Fleischstraße 77
Telefon: (0651) 48 802
trier@vz-rlp.de

55543 Bad Kreuznach
(Kreisverwaltung)
Salinenstr. 47
bad-kreuznach@vz-rlp.de

57518 Betzdorf (Rathaus),
Hellerstraße 2
betzdorf@vz-rlp.de

56812 Cochem (Kreisverwaltung),
Brückenstr. 2
cochem@vz-rlp.de

76727 Germersheim
(Kreisverwaltung), Luitpoldplatz 1
germersheim@vz-rlp.de

57627 Hachenburg (Rathaus),
Gartenstr. 11
hachenburg@vz-rlp.de

76829 Landau (Kreisverwaltung),
Luitpoldplatz
landau@vz-rlp.de

54595 Prüm, (Konvikt – Haus der Kultur), Kalvarienbergstr. 1
pruem@vz-rlp.de

55469 Simmern (Kreisverwaltung),
Ludwigstraße 3–5
simmern@vz-rlp.de

verbraucherzentrale

Rheinland-Pfalz

Wissen, was wirklich Sache ist.

Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10
55116 Mainz
Telefon (06131) 28 48 0
Telefax (06131) 28 48 66
info@vz-rlp.de
www.verbraucherzentrale-rlp.de

Für den Inhalt verantwortlich: Ulrike von der Lüche, Vorstand
Redaktion: Lore Herrmann-Karch
Foto: ©iStock.com/YakobchukOlena,
USA Reiseblogger/pixabay
Stand: 10/2020

gefördert durch:



verbraucherzentrale

Rheinland-Pfalz

Wissen, was wirklich Sache ist.

MIT WLAN DRAHTLOS INS INTERNET

Richtig absichern –
Kosten und Missbrauch vermeiden

❖❖❖ WAS IST WLAN?

WLAN steht für Wireless Local Area Network.

So nennt man den drahtlosen Zugang ins Internet. Damit können Sie heute bequem vom Balkon oder dem Garten – ganz ohne lästige Kabelverbindung – im Internet surfen. Allerdings sollten Sie Ihren drahtlosen Internetzugang immer sorgfältig gegen unbefugtes Nutzen absichern.

❖❖❖ WARUM ABSICHERN?

Als Anschlussinhaber sind Sie grundsätzlich für einen möglichen Missbrauch Ihres Internetanschlusses durch unbefugte Dritte verantwortlich.

Loggt sich beispielsweise ein Fremder ein und begeht in einer Tauschbörse eine Urheberrechtsverletzung, so haften Sie möglicherweise dafür. Dies kann für Sie unter Umständen sehr teuer werden.

Eine hundertprozentige Sicherheit, Ihr WLAN gegen unbefugte Dritte abzusichern, gibt es nicht. Es geht vielmehr darum, es einem möglichen Angreifer besonders schwer zu machen.



ACHTUNG:

Bei einem unverschlüsselten WLAN sind Sie als Anschlussinhaber grundsätzlich für einen möglichen Missbrauch Ihres Internetanschlusses durch unbefugte Dritte verantwortlich.

❖❖❖ BENUTZEROBERFLÄCHE STARTEN

Für das drahtlose Surfen benötigen Sie einen WLAN-Router. Er ermöglicht, eine Internetverbindung auf mehrere Geräte, beispielsweise PC, Laptop, Smartphone oder Tablet zu verteilen.

Handelsübliche Router können über eine sogenannte grafische Benutzeroberfläche mit dem Webbrowser, z. B. Internet Explorer oder Firefox, eingerichtet werden. Um den Router einzurichten, müssen Sie in die Adresszeile des Webbrowsers die IP-Adresse des Routers eingeben, z. B. 192.168.1.1. Manche Router können auch über ein Schlüsselwort wie fritz.box, speedport.ip erreicht werden. Ein Hinweis auf die Zugangsdaten des Routers findet sich in der Bedienungsanleitung, bei manchen Geräten auch auf der Rückseite. Die meisten Router haben zudem ein Passwort für die Benutzeroberfläche, z. B. 0000, admin, password.

Da dieses voreingestellt ist, sollten Sie es auf jeden Fall ändern. Bei manchen Routern ist für die Einrichtung oder die Änderung der Einstellungen eine Internetverbindung über ein Netzwerkkabel (LAN) notwendig.

❖❖❖ WLAN VERSCHLÜSSELN

Im nächsten Schritt sollten Sie Ihr WLAN verschlüsseln.

Manche Router sind werkseitig auf „unverschlüsselt“ eingestellt. Bei anderen ist eine WEP-Verschlüsselung oder eine WPA/WPA2-Verschlüsselung vorhanden. Die WEP-Verschlüsselung kann sehr leicht geknackt werden. Stellen Sie daher immer die WPA bzw. WPA2-Verschlüsselung ein. Sie ist der heute gängigste Verschlüsselungsstandard. Inzwischen gibt es mit WPA3 auch schon einen Nachfolgestandard, der allerdings momentan nur von sehr wenigen Geräten unterstützt wird.



ACHTUNG:

Stellen Sie immer mindestens die WPA bzw. WPA2-Verschlüsselung ein. Falls möglich, stellen Sie die WPA3 Verschlüsselung ein.



❖❖❖ RICHTIGES PASSWORT FÜR DIE VERSCHLÜSSELUNG

Ein sicheres Passwort sollte mindestens aus zwanzig Zeichen bestehen – gemischt aus Buchstaben, Zahlen und Sonderzeichen.

Zudem sollte man bei Buchstaben zwischen Groß- und Kleinschreibung variieren und das Passwort sollte keinen Sinn ergeben.

❖❖❖ WLAN NAME

Jedes WLAN hat einen Namen, eine sogenannte SSID (Set Service Identifier).

Der Name wird standardmäßig vom Hersteller vergeben, meist wird auch die Gerätebezeichnung verwendet. Diesen Namen sollten Sie individuell verändern, jedoch sollte der neue WLAN Name keine Rückschlüsse auf Sie als Besitzer zulassen, z. B. MeyerWLAN.

Bei vielen Routern haben Sie die Möglichkeit, die Übermittlung der SSID zu unterdrücken. Dies hat den Vorteil, dass ein unbefugter Dritter, der auf Ihr WLAN zugreifen will, nicht nur das Passwort des WLANs ausspähen muss, sondern auch noch den Namen des WLANs.

❖❖❖ MAC ADRESSFILTERUNG

Neben dem Router ist noch eine WLAN-Netzwerkkarte erforderlich.

Jede Netzwerkkarte und auch jede WLAN-Karte hat eine sogenannte MAC Adresse (Media Access Control). Diese hat nichts mit dem Macintosh-Computer zu tun. Die MAC Adresse ist vielmehr vergleichbar mit der Fahrgestellnummer eines PKW.

Sie ist eindeutig und nur ein einziges Mal vergeben. Viele WLAN-Router bieten die Möglichkeit der Filterung, d. h. nur bekannte MAC Adressen, also bekannte WLAN-Rechner werden für eine WLAN-Verbindung zugelassen. Bei manchen Herstellern wird die MAC Adresse auch als „Physikalische Adresse“ bezeichnet.

❖❖❖ IP-ADRESSRAUM UND DHCP FUNKTION BEGRENZEN

Die sog. DHCP Funktion (Dynamic Host Configuration Protocol) des Routers vergibt die sogenannten IP-Adressen automatisch an die angeschlossenen Geräte.

Jedes angeschlossene Gerät erhält somit vom Router eine IP-Adresse zum Internetsurfen. Werkseitig sind Router so eingestellt, dass theoretisch bis zu 256 Geräte angeschlossen werden könnten. Diese hohe Anzahl sollten Sie auf die tatsächliche Anzahl der von Ihnen angeschlossenen Geräte (Clients) reduzieren. Fortgeschrittene Benutzer können auch die DHCP-Funktion komplett abschalten und die IP-Adresse manuell an jedem PC vergeben.

❖❖❖ FILTER

Viele Router bieten die Möglichkeit, einzelne Dienste zu sperren, wie beispielsweise Filesharing.

Damit wird verhindert, dass ein Nutzer ggf. urheberrechtlich geschützte Dateien wie Musik oder Filme herunterladen kann.

❖❖❖ GASTNETZ

Wer seinen Gästen die WLAN-Nutzung ermöglichen will, kann dies über ein WLAN-Gastnetz tun.

Das Gastnetz ist ein separates WLAN und verhindert, dass der Gast auf das heimische Netzwerk zugreifen kann.

❖❖❖ KINDERSICHERUNG

Viele WLAN-Router verfügen auch über eine Kindersicherung.

Diese ist eigentlich dazu gedacht, die Internetnutzung für Kinder über spezielle Zugangsregeln zu beschränken. Allerdings kann man diese Zugangsregeln auch so einstellen, dass allen bekannten (und erlaubten) Rechnern die Internetnutzung freigegeben wird, bei neu hinzukommenden Rechnern jedoch die Kindersicherung eingreift und eine Internetnutzung nicht erlaubt ist.

