

An die ehrenamtlichen Helfer
und Helferkreise

Almersweg 10
82205 Gilching

Tel. 0163 / 7728818
Mail: vw@refugees-online.de
Web: www.refugees-online.de

Vorstand:
Volker Werbus (1. Vors.)
Helga Werbus (2. Vors.)

Internetzugang für Flüchtlinge

Wie Sie helfen können – was Sie beachten müssen

Gilching, im Mai 2020

Sehr geehrte Helfer*innen,

unser Verein kümmert sich um die Bereitstellung von Internet und PCs für Flüchtlinge. Was Anfang 2015 als engagiertes Einzelprojekt in der Erstaufnahme in Fürstenfeldbruck begonnen hat ist zu etwas viel Größerem gewachsen. Dank der Hilfe und Mitarbeit vieler ehrenamtlicher Helfer sind wir mittlerweile in über 160 Einrichtungen aktiv.

Sie möchten auch etwas tun oder suchen den Erfahrungsaustausch mit uns. Das ist schön.

Bitte beachten Sie: Wir können Ihnen kein „mundgerechtes“ Hilfsprojekt liefern. Sie müssen sich „Ihr“ Aufgabengebiet und „Ihr“ Projekt suchen. Oder Sie haben vielleicht schon eines. Dann können wir Ihnen mit dem nachstehenden Dokument helfen und ggf. viel Arbeit ersparen.

Wir arbeiten sehr intensiv mit dem Verein AsylPlus e.V. zusammen (www.asylplus.de). Der Verein hat eine ganz wunderbare Online-Lernplattform zusammengestellt, die nahezu alle Bereiche von der Alphabetisierung bis zum Hochschulstudium abdeckt und die Asylbewerber hilft, sich in Deutschland zu integrieren und ein selbstbestimmtes Leben aufzubauen. Und die Menschen, die in Ihre Heimatländer zurückkehren werden, können sich Fertigkeiten und Kenntnisse aneignen die auch später sehr nützlich sein werden.

Die Kooperation mit weiteren Vereinen wurde unter dem Dach „Chancen Plus“ (www.chancenplus.de) weiter ausgebaut.

Wir haben Ihnen auf den nachfolgenden Seiten reichlich „Lesestoff“ zusammengestellt. Da wir Ihre technischen Vorkenntnisse nicht kennen, sind wir an vielen Stellen sehr weit ins Detail gegangen. Die von uns vorgeschlagene Lösung wurde über die Jahre ständig verbessert und hat sich in den vielen Projekten bestens bewährt.

Wir wünschen Ihnen bei der Lektüre viel Spaß und freuen uns auf die Zusammenarbeit mit Ihnen.

Es grüßen Sie ganz herzlich,

Waldtraut Haase (AsylPlus e.V.) und Volker Werbus (Refugees Online e.V.)

Störerhaftung, WLAN-Hotspot-System, benötigte Infrastruktur

Der Gesetzgeber hat das Telemedien-Gesetz novelliert und die vorgeschlagenen Änderungen sind am 13.10.2017 in Kraft getreten.

<http://aspvr.de/offenes-wlan-und-stoererhaftung-die-reform-des-telemediengesetzes-tmg/>

Damit entfällt die so genannte „Störerhaftung“, bei der Betreiber von WLAN-Diensten für Verstöße Dritter in die Haftung genommen werden können. Internet-Anschlüsse für Asylbewerber-Unterkünfte können nun weitgehend risikolos auch von Helfern bereitgestellt werden. Bislang waren nur die Provider von der Haftung freigestellt, der Gesetzgeber hat nun auch den Anschluss-Inhaber vor kostenpflichtigen Abmahnungen weitgehend befreit. Ausnahmen bestehen nur noch, wenn der Anschlussinhaber *„absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen“*.

Wir setzen in den Unterkünften ein professionelles WLAN-Hotspot-System ein und nutzen den Jugendschutz-Filter der Bundesprüfstelle für jugendgefährdende Medien. Der Einsatz eines Hotspot-Systems hat mehrere Vorteile: Zum einen wird die vorhandene Bandbreite des Anschlusses gerechter auf die Nutzer aufgeteilt, zum anderen kann durch die Ausgabe der individuellen Zugangscodes auch eine Kostenbeteiligung der Nutzer umgesetzt werden.

Gerne stellen wir Ihnen ein solches Hotspot-System zu Selbstkosten zur Verfügung.

Wir empfehlen den Einsatz eines solchen Systems ab 20 Bewohnern, bei weniger Bewohnern (z.B. in dezentralen, kleineren Unterkünften) reicht eine entsprechend unseren Hinweisen konfigurierte Fritzbox. (siehe Abschnitt „Konfiguration der Fritzbox“)

Um eine Unterkunft mit WLAN auszurüsten müssen in der Regel mehrere Access Points aufgestellt werden. Diese Access Points werden über ein LAN miteinander verbunden. Da in den Unterkünften meist kein solches LAN vorhanden ist, muss es aufgebaut werden. Dabei sind einige Dinge zu beachten: In den Unterkünften darf zumeist nichts fest installiert werden (keine Leitungen verlegen, keine Löcher bohren, etc.) Daher setzen wir auf Technologien, die auch ohne aufwändige Installation ein solches LAN bilden. Je nach den örtlichen Gegebenheiten sind das meist Powerline-Adapter oder spezielle Flachbandkabel, die man beschädigungsfrei durch die Fensterrahmen verlegen kann. Unterkünfte ohne eigenen DSL-Anschluss binden wir wo es möglich ist über Richtfunk an.

Der Brandschutz muss ebenfalls beachtet werden, so dürfen in den Fluchtwegen (Flure, Treppenhäuser) keine Access Points aufgestellt werden.

Bitte beachten Sie: Sie benötigen für den Betrieb von Internetleitungen in Flüchtlingsunterkünften immer eine Genehmigung des Betreibers der Unterkunft!

Wie funktioniert das WLAN-Hotspot-System?

Wir nutzen Systeme auf der Basis der Open-Source-Software PFSense (www.pfsense.org)
Diese Software ist bewährt, extrem stabil und lässt sich durch den Einsatz auf verschiedenen Hardware-Plattformen sehr gut skalieren.

Wir haben für verschieden große Unterkünfte Standard-Kombinationen ausgearbeitet, die alle nach dem nachfolgend beschriebenen Prinzip arbeiten:

Nutzer, die sich mit dem WLAN verbinden und ins Internet gehen wollen, werden zunächst auf eine Portalseite umgeleitet. Dort muss ein so genannter Vouchercode eingegeben werden und dann wird der Internetzugang freigeschaltet.

Sie bekommen von uns zusammen mit dem System PDF-Dateien mit Vouchercodes. Diese sind durchnummeriert und werden nach Bedarf ausgedruckt und den Nutzern ausgehändigt. Notieren Sie in jedem Fall die laufende Nummer des Vouchers und den Namen (und ggf. die Ausweis -Nummer) des Nutzers in einer Ausgabeliste und lassen ihn/sie die beigefügte Erklärung unterschreiben. Mit dem Vouchercode können sich die Nutzer einloggen und den Internetservice nutzen.

Damit niemand unnötig Kapazität blockieren kann, erfolgt nach 2 Stunden Inaktivität automatisch ein Logout. Daher ist ein explizites Ausloggen nicht notwendig. Der Nutzer kann sich natürlich wieder neu einloggen.

Die Voucher gelten für 30 Tage und sind nach Ablauf dieser Zeit gesperrt. Der Nutzer muss sich dann einen neuen Code holen. Sollten Sie eine andere Gültigkeitsdauer wünschen, sagen Sie uns das bitte. Das System protokolliert jeden Login- und Logout-Vorgang mit IP-Adresse, Vouchercode und MAC-Adresse des Geräts. Das Surfverhalten wird **nicht** protokolliert. Die Protokolle werden lokal auf dem System gespeichert und zusätzlich auf einen unserer Server kopiert.

Je nach verfügbarer Bandbreite kann man die jedem einzelnen Nutzer zugewiesene Bandbreite begrenzen und eine gleichmäßige Verteilung auf alle Nutzer sicherstellen. Erfahrungsgemäß muss man dies nur bei Leitungen mit 16 Mbit/s oder weniger einrichten. Schnelle VDSL-Anschlüsse oder Kabel-Internet haben meist ausreichend Bandbreite, so dass auf eine Begrenzung verzichtet werden kann.

Bei der Aufstellung des Systems ist es wichtig, dass die zentralen Komponenten (Fritzbox, Hotspot-System) für die Nutzer nicht zugänglich sind, also entweder in einem abschließbaren Schrank oder einem abschließbaren Raum aufgestellt sind.

Welche Systeme für welche Nutzeranzahl?

Für Unterkünfte mit nur wenigen Bewohnern reicht es aus, eine verschlüsselte Fritzbox aufzustellen und statt des Vouchercodes den WLAN-Schlüssel herauszugeben. Bei Bedarf kann man diesen monatlich ändern und so Missbrauch durch unbefugte Weitergabe des WLAN-Schlüssels vermeiden oder zumindest erschweren.

Für Unterkünfte zwischen 20 und 100 Nutzern reicht eine kleine Alix-Box mit integriertem WLAN oder einigen wenigen Access Points aus. Das Gerät trägt die Bezeichnung **Alix2D13** und kann bei uns fertig konfiguriert für rund 200 Euro erworben werden. Um Kosten zu sparen erwerben wir immer

wieder mal gebrauchte Geräte oder kaufen Restposten. Diesen Kostenvorteil geben wir an die Helfer weiter. Falls Sie die Alix-Box lieber selber zusammenbauen und konfigurieren wollen geben wir Ihnen gerne die Stückliste und die Bezugsquelle.

Für Unterkünfte mit mehr als 100 Nutzern empfehlen wir den Einsatz einer leistungsfähigeren Box, der **APU1D4**, oder eines Servers. Da es hier sehr viele unterschiedliche Geräte gibt, müssen wir von Fall zu Fall schauen welche Hardware verfügbar ist. Bislang haben wir Panel-PCs von AAEON und AFL sowie 19“-Pyramid-Server im Einsatz.

Das Hotspot-System wird immer nach folgendem Schema angeschlossen:



Die Alix- oder APU-Boxen haben keinerlei bewegte Teile und können problemlos auch in einem geschlossenen Schrank ohne Lüftung aufgestellt werden. Die Leistungsaufnahme liegt bei wenigen Watt und die Geräte entwickeln nur ganz wenig Wärme.

Access Points










Wir empfehlen den Einsatz von gebrauchten Access Points, die Sie für wenig Geld bei Ebay oder zu Selbstkosten bei uns beziehen können. Wir haben anfangs meist Cisco Aironet 1231G eingesetzt, die sind für rund 60 Euro erhältlich. Mittlerweile gibt es auch preisgünstige gebrauchte Dual-Band Access Points, hier hat sich der Ruckus 7363 im Einsatz bewährt. Im Gegensatz zu dem Cisco hat der Ruckus einen eingebauten Switch und kann damit auch wunderbar kaskadiert werden.

In Unterkünften, in denen viele Access Points benötigt werden (z.B. in Container-Wohnanlagen) kann man auf preiswertere Access Points ausweichen. Wir setzen zumeist zum Access Point umkonfigurierte WLAN-Router ein. Diese haben ebenfalls einen eingebauten LAN-Switch und lassen sich ohne großen Aufwand kaskadieren.

Betrieb und Wartung

Die Geräte sind allesamt fernüberwacht und auch aus der Ferne wartbar. Falls mal vor Ort eingegriffen werden muss beschränkt sich das meist auf einen „Power-On-Reset“, also das simple Ziehen und wieder Einstecken des Strom-Anschlusskabels.

Der Status der Geräte ist bequem im Internet abrufbar, die entsprechende Webseite für „ihre“ Unterkunft richten wir Ihnen gerne ein.

Status	Last 7 days		Type	02 May	01 May	30 Apr	29 Apr	28 Apr	27 Apr	26 Apr
	100.00%	AP10 Haus 2a aussen	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	100.00%	AP11 Haus 4 Whg. 3 EG (n...	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	100.00%	AP12 Haus 4 Whg. 5 EG	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	0.000%	AP2 Haus 2a EG	port	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	100.00%	AP3 Haus 2a OG	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	99.986%	AP4 Haus 2b EG	port	100.00%	100.00%	100.00%	100.00%	99.903%	100.00%	100.00%
	100.00%	AP5 Haus 2b OG	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	100.00%	AP6 Haus 4 Whg.1 EG	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	100.00%	AP7 Haus 4 Whg. 2 OG	port	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

Ein paar Gedanken zu Vouchercodes und Internetleitungen

Die Vouchercodes sind kostenlos, wir liefern Ihnen als „Erstausrüstung“ 1.000 Stück mit. Sie können immer wieder bei uns nachbestellen, auch die Nachbestellungen sind kostenlos.

Einige Helferkreise „verkaufen“ die Vouchercodes an die Nutzer und decken so die Kosten der Internetleitung. Das ist ok, solange niemand etwas daran verdient. Als gemeinnütziger Verein müssen wir darauf achten. Sollten wir feststellen dass unsere Systeme missbräuchlich zu gewerblichen Zwecken genutzt werden, beenden wir die Zusammenarbeit mit dem jeweiligen Helferkreis mit sofortiger Wirkung und behalten uns vor, die von uns gelieferten Voucher im System zu löschen und damit ungültig zu machen.

Die WLAN-Kennung ist standardmäßig „RefugeesOnline“. Da sich auch alle Anleitungen darauf beziehen würden wir das ungern ändern. Das führt sonst nur zu Verwirrung bei den Nutzern oder zu Mehrarbeit bei uns, wenn wir dann für diese Fälle sozusagen eine eigene Dokumentation anfertigen müssten.

Die Internetleitung sollte der Helferkreis stellen. Grundsätzlich geht jeder Provider, klären Sie aber bei der Bestellung ab, ob eine Mehrfachnutzung zulässig ist. Wir hatten bisher noch keine Probleme, wir arbeiten vorwiegend mit 1&1 und M-Net zusammen.

Achten Sie bitte auf möglichst kurze Vertragslaufzeiten. Falls mal eine Unterkunft geschlossen wird (das hatten wir schon mehrfach) bleibt man dann nicht auf einem nutzlosen Vertrag sitzen.

Projektablauf

Ein typischer Projektablauf sieht folgendermaßen aus:

Der Helferkreis holt sich eine Genehmigung zur Errichtung eines WLAN in einer Unterkunft vom Betreiber ein. Dabei können wir gerne unterstützen, viele Bezirksregierungen und Landratsämter kennen uns bereits gut. Dann werden uns folgende Daten übermittelt:

- Genaue Anschrift der Unterkunft
- Lage des Telefonanschlusses im Gebäude
- Anzahl der Nutzer

- Beschreibung der baulichen Gegebenheiten (Bauweise, Grundriss-Skizze)
- Vorhandene Infrastruktur (LAN, Telefonkabel etc.)

Wir machen dann eine Planung und eine Kostenabschätzung für die Hardware. Dann kann der Helferkreis entscheiden, ob das umgesetzt werden soll. Die Geräte liefern wir anschlussfertig per Post zusammen mit einer Anleitung zum Aufstellen der Geräte.

Wir stellen eine Rechnung für die entstandenen Hardware-Kosten. Unsere Arbeit (Planung, Beschaffung und Konfiguration der Hardware, Fernwartung, etc.) erbringen wir ehrenamtlich.

Kommunikation mit den Bewohnern

Wir haben in den meisten Unterkünften ein „elektronisches Schwarzes Brett“ eingerichtet, das ist eine Webseite auf die jeder Nutzer nach dem Einloggen weitergeleitet wird. Die Seite ist ganz einfach zu administrieren, das geht online über das Internet und alle Aktualisierungen erscheinen nach wenigen Sekunden in der Unterkunft.



Wichtige Informationen
<p>Kathrin (Caritas) Handy: 01875 4890376 Email: kathrin.hiem@caritasmuenchen.de</p>
<p><i>Information zu Corona</i></p> <p>deutsch: https://www.muenchen.de/rathaus/Stadinfos/Presse-Service/Presse-Archiv/2020/Coronavirus/informationen-zum-Corona-Virus-in-Leichter-Sprache.html https://handbookgermany.de/de/live/coronavirus.html</p> <p>english: https://handbookgermany.de/en/live/coronavirus.html</p> <p>قوروننا (COVID-19) https://handbookgermany.de/ar/live/coronavirus.html</p> <p>قوروننا ویروس در آلمان (COVID-19) https://handbookgermany.de/fa/live/coronavirus.html</p>
<p><i>Du willst deine Meinung zur Situation im Heim weitergeben?:</i></p> <p>Online-Umfrage des Münchner Flüchtlingsrat: https://lamapoll.de/Situation-mit-Corona/ auf Englisch, Französisch, Arabisch und Farsi</p>
<p>Deutschkurs in Frankfurter Straße</p> <p style="background-color: red; color: white; text-align: center;">ABGESAGT - KEIN DEUTSCHKURS wegen Corona</p>

Kommunikation mit uns

Alle Vereinsmitglieder stehen noch im Berufsleben und arbeiten in Ihrer Freizeit für den Verein. Unser bevorzugter Kommunikationsweg ist daher **E-Mail**. Wir können tagsüber neben unseren Berufen nicht noch Dutzende von Telefonaten führen. Gerne vereinbaren wir per E-Mail Termine mit Ihnen für ein Telefonat. Danke für Ihr Verständnis.

Weitere Informationen

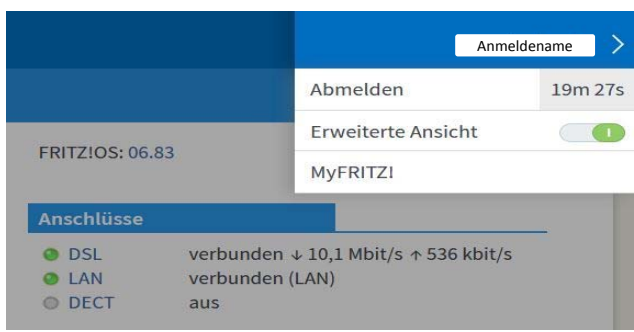
Neben unserer Webseite www.refugees-online.de pflegen wir auch ein kleines „Tagebuch“ auf Facebook. Besuchen Sie uns doch mal dort: www.facebook.com/refugeesonline

Programmierung einer Fritz!Box für Hotspot-Systeme

Damit das von uns zur Verfügung gestellte Hotspot-System funktioniert und auch von uns über das Internet gewartet werden kann sind einige Einstellungen nötig. Diese Einstellungen zeigen wir Ihnen nachstehend beispielhaft.

Wichtig: Lassen Sie alle Einstellungen der Fritzbox bitte zunächst auf den werksseitig voreingestellten Werten. Die betrifft insbesondere die IP-Einstellungen für das Heimnetz.

Bevor Sie mit der Programmierung beginnen, stellen Sie die Fritzbox bitte auf „Erweiterte Ansicht“. Klicken Sie dazu oben rechts auf Ihren Anmeldenamen, es öffnet sich folgendes Fenster:



Richten Sie bitte einen neuen bzw. zusätzlichen Fritzbox-Benutzer ein. Dazu sind 3 Angaben nötig: Ein Benutzername (frei wählbar), eine E-Mail-Adresse (bitte vw@refugees-online.de eintragen) und ein Passwort. Das Passwort ist frei wählbar. Teilen Sie uns das Passwort bitte mit – wir benötigen es für den Fernzugriff auf Ihre Fritzbox.



Ändern Sie den https-Port für die Fernwartung der Fritzbox auf 455 (der Standard-Port 443 wird für das Hotspot-System genutzt) und geben Sie die Fernwartung frei.

The screenshot shows the 'FRITZ!Box 7412' web interface. The left sidebar contains navigation options: Übersicht, Internet, Online-Monitor, Zugangsdaten, Filter, Freigaben (highlighted), MyFRITZ!-Konto, DSL-Informationen, Telefonie, Heimnetz, and DECT. The main content area is titled 'Internet > Freigaben' and has tabs for 'Portfreigaben', 'FRITZ!Box-Dienste', 'DynDNS', and 'VPN'. Under 'FRITZ!Box-Dienste', the 'TCP-Port für HTTPS' section is active. It explains that the Fritz!Box uses a specific TCP port for HTTPS and allows changing it. The 'TCP-Port für HTTPS' is set to 455 (circled in red), with a note '(im Bereich von 1 bis 65535)'. Below, the 'Heimnetzadresse Ihrer FRITZ!Box' is shown as 'https://fritz.box:455' or 'https://192.168.178.1:455'. A note states: 'Unter diesen Adressen ist Ihre FRITZ!Box aus dem Heimnetz über HTTPS erreichbar.' In the 'Internetzugriff' section, the checkbox 'Internetzugriff auf die FRITZ!Box über HTTPS aktivieren' is checked (circled in red). A note below explains: 'Diese Option ermöglicht den Zugang auf die FRITZ!Box aus dem Internet. Zugang haben alle FRITZ!Box-Benutzer, denen im Menü "System > FRITZ!Box-Benutzer" das Recht "Zugang auch aus dem Internet erlaubt" eingeräumt'.

Damit die Fritzbox bei wechselnden IP-Adressen des Anbieters zuverlässig erreichbar ist, richten Sie bitte einen DynDNS-Account ein. Wir empfehlen den kostenlosen Dienst von www.spdyn.de. Tragen Sie Ihren Account entsprechend ein und teilen uns die Domain mit. Gerne bereiten wir Ihnen auch einen DynDNS-Account vor, fragen Sie uns bitte danach.

The screenshot shows the 'FRITZ!Box 7412' web interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Internet > Freigaben' and has tabs for 'Portfreigaben', 'FRITZ!Box-Dienste', 'DynDNS', and 'VPN'. Under 'DynDNS', the 'DynDNS benutzen' checkbox is checked. A note explains: 'Über DynDNS können Anwendungen und Dienste, für die in der FRITZ!Box-Firewall Portfreigaben eingerichtet wurden, unter einem festen Domainnamen aus dem Internet erreicht werden, obwohl sich die öffentliche IP-Adresse der FRITZ!Box mit jeder Interneteinwahl ändert.' Below, the 'Geben Sie die Anmeldedaten für Ihren DynDNS-Anbieter an.' section is shown. The 'DynDNS-Anbieter' is set to 'Benutzerdefiniert'. The 'Update-URL' is 'update.spdyn.de/nic/update?hostnam'. The 'Domainname' is 'Domain.spdns.org'. The 'Benutzername' is 'refugeesonline' and the 'Kennwort' is masked with dots.

Um File-Sharing-Dienste zu sperren und den Jugendschutz-Filter zu aktivieren bearbeiten Sie bitte das unter „Filter“ Profil „Standard“ und aktivieren die Seiten-Filterung. Dazu bitte auf das Bleistift-Symbol links neben dem roten X am rechten Rand der Zeile mit dem Standard-Profil klicken.

FRITZ!Box 7412 MyFRITZ! Anmeldenname

Internet > Filter

Kindersicherung | **Zugangsprofile** | Priorisierung | Listen

Zugangsprofile

Mithilfe der Zugangsprofile legen Sie fest, wie die Netzwerkgeräte das Internet nutzen dürfen. Einige Profile sind bereits angelegt. Bei Bedarf können Sie diese bearbeiten und weitere Profile hinzufügen.

Name	Online-Zeit	Geteiltes Budget	Filter	Gesperrte Anwendungen	
Gast	unbegrenzt	—	Blacklist, BPjM	alles außer Surfen und Mailen	
Gesperrt	keine	—	—	—	
Standard	unbegrenzt	—	Blacklist, BPjM	FTP-Server, eMule, BitTorrent, MS Remote Desktop, Telnet	
Unbeschränkt	unbegrenzt	—	—	—	

FRITZ!Box 7412 MyFRITZ! Anmeldenname

Zugangsprofil Standard bearbeiten

Filter für Internetseiten

Hier können Sie festlegen, ob und welche Internetseiten für dieses Zugangsprofil gefiltert werden.

Internetseiten filtern

Filterlisten

- Internetseiten erlauben (Whitelist) (Liste anzeigen)
Nur die Internet-Adressen, die in der Whitelist enthalten sind, können aufgerufen werden.
- Internetseiten sperren (Blacklist) (Liste anzeigen)
Alle Internet-Adressen, die in der Blacklist enthalten sind, sind gesperrt.
Aufrufe über IP-Adressen sind ebenfalls gesperrt. (Ausnahmen anzeigen)
- jugendgefährdende Internetseiten sperren (BPjM-Modul)
Zusätzlich werden die von der BPjM indizierten Internetseiten gefiltert.

Hinweis:
Die Filterlisten Whitelist und Blacklist können Sie im Bereich Internet > Filter > Listen lesen und bearbeiten.

Tragen Sie die zu sperrenden Dienste aus dem Drop-Down-Menü ein. Lassen Sie die Dienste HTTP-Server und SSH bitte ungesperrt!

FRITZ!Box 7412 MyFRITZ! Anmelden

Zugangsprofil Standard bearbeiten

Gesperrte Netzwerkanwendungen

Legen Sie hier fest, für welche Netzwerkanwendungen die Internetnutzung für dieses Zugangsprofil gesperrt sein soll.

Netzwerkanwendung	entfernen
Telnet	X
MS Remote Desktop	X
FTP-Server	X
eMule	X
BitTorrent	X

Netzwerkanwendung sperren: Bitte wählen ...

Hinweis:
Um weitere Netzwerkanwendungen in der Auswahl zu ergänzen, müssen Sie diese zuvor im Bereich Internet > Filter > Listen definieren.

Tragen Sie bitte die im Bild unten angegebenen Portweiterleitungen für die Fernwartung ein. Die Ports müssen auf die IP-Adresse 192.168.178.2 weitergeleitet werden:

FRITZ!Box 7412 MyFRITZ! Anmelden

Internet > Freigaben

Alle mit der FRITZ!Box verbundenen Geräte sind vor unerwünschten Zugriffen aus dem Internet geschützt. Einige Anwendungen, wie z.B. Online-Spiele, müssen jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Einrichtung von Portfreigaben können Sie solche Verbindungen erlauben.

Gerät / Name	IP-Adresse	Freigaben	Port extern vergeben IPv4	Selbstständige Portfreigabe
PC-192-168-178-2	192.168.178.2	<ul style="list-style-type: none">PFSensePFSense SSHAPs	<ul style="list-style-type: none">4432250002 - 50020	<input type="checkbox"/> 0 aktiv

Gerät für Freigaben hinzufügen Aktualisieren

Sie können die Einstellung "Selbstständige Portfreigabe" für alle Geräte deaktivieren, die bisher keine Portfreigabe angefordert haben.

Sofern der verschlüsselte WLAN-Zugang zur Fritzbox nicht benötigt wird, schalten Sie WLAN aus.

Richten Sie den oder die am Hotspot angeschlossenen Access Point so ein, dass er/sie entweder eine feste IP-Adresse zwischen 192.168.99.2 und 192.168.99.19 bekommt/bekommen oder die Adresse(n) über DHCP bezieht.

Ändern Sie die SSID des Access Points auf „RefugeesOnline“ und lassen Sie diesen Zugang **unverschlüsselt**. Das ist zulässig, weil der Zugang ohnehin nur mit gültigem Vouchercode möglich ist. Viele Geräte können sich bei unverschlüsseltem Zugang meist schneller verbinden und Ihre Nutzer müssen nicht noch zusätzlich zum Vouchercode einen WLAN-Key eingeben.

Gerne sind wir Ihnen bei der Programmierung der Fritzbox oder des Access Point behilflich.

Wir setzen meist gebrauchte Access Points von Cisco ein (Aironet 1231G).
Ein Konfigurations-File für den Cisco senden wir Ihnen gerne zu.

Auch ein „alter“ WLAN-Router kann zum Access Point umfunktioniert werden.

Wichtig ist hier nur, dass der Access Point die Adresse 192.168.99.2 oder DHCP hat und das bei Verwendung eines alten Routers der lokale DHCP-Server deaktiviert ist.

Hinweis für Internetzugänge mit IPv6 oder IPv6-DS-Lite: Unsere Fernwartung ist zwar auch IPv6-fähig, die Einrichtung ist aber ungleich komplexer. Daher beantragen Sie bitte bei Ihrem Provider eine IPv4-Adresse. Die meisten Provider bieten diesen Service kostenlos an.

Für Rückfragen nutzen Sie bitte die E-Mail-Adresse support@refugees-online.de

Konfiguration der Fritzbox für weniger als 20 Nutzer

Grundsätzlich gilt: Die Verschlüsselung ist nur über WLAN bzw. den WLAN-Gastzugang wirksam. Die LAN-Anschlüsse sind unverschlüsselt. Stellen Sie das Gerät daher am besten so auf, dass die Nutzer keinen Zugang zu den LAN-Ports haben.

Der Zugang zur Administrationsoberfläche der Fritz!Box sollte durch ein Passwort geschützt werden, das nur Ihnen bekannt ist.

The screenshot shows the configuration page for a Fritz!Box 7360. The main navigation bar at the top includes the Fritz! logo and the model name 'FRITZ!Box 7360'. Below this, there are links for 'FRITZ!Box', 'FRITZ!NAS', and 'MyFRITZ!'. On the left side, there is a sidebar menu with categories: 'Übersicht', 'Internet', 'Telefonie', 'Heimnetz', 'WLAN', 'DECT', 'Diagnose', and 'System'. Under 'WLAN', sub-items include 'Funknetz', 'Funkkanal', 'Sicherheit', 'Zeitschaltung', 'Gastzugang', and 'Repeater'. The 'Sicherheit' section is currently selected. It has two tabs: 'Verschlüsselung' (active) and 'WPS-Schnellverbindung'. The main text reads: 'Legen Sie hier fest, wie Ihr WLAN-Funknetz gegen unberechtigte Nutzung und gegen Abhören gesichert werden soll.' Below this are three radio button options: 'WPA-Verschlüsselung (größte Sicherheit)', 'WEP-Verschlüsselung (nicht empfohlen, unsicher)', and 'unverschlüsselt (nicht empfohlen, ungeschützt)'. The 'WPA-Verschlüsselung' option is selected. Below this is the 'WPA-Verschlüsselung' section, which says: 'Legen Sie einen WLAN-Netzwerkschlüssel fest. Mit diesem WLAN-Netzwerkschlüssel werden die WLAN-Verbindungen gesichert. Der Netzwerkschlüssel muss zwischen 8 und 63 Zeichen lang sein.' There are two fields: 'WPA-Modus' with a dropdown menu set to 'WPA + WPA2', and 'WLAN-Netzwerkschlüssel' with an empty text input field. A red arrow points to the input field.

Werkseitig ist der WLAN-Zugang bereits verschlüsselt. Der Schlüssel ist auf einem Aufkleber hinten auf der Fritz!Box notiert. Ändern Sie diesen Schlüssel in diesem Feld. Notieren Sie sich den geänderten Schlüssel und bewahren Sie die Notiz gut auf. Speichern Sie Ihre Eingabe durch anklicken des Buttons am Seitenende.

Geben Sie diesen Schlüssel **nicht** an die Nutzer heraus, dazu ist der WLAN-Gastzugang gedacht, dazu kommen wir im nächsten Schritt.

Aktivieren Sie nun den Gastzugang der Fritzbox.

Klicken Sie die Box „Gastzugang aktiv“ sowie die Box „Internetanwendungen beschränken“ und geben Sie einen Schlüssel für das Gast-WLAN in dieses Feld ein. Werkseitig steht da bereits ein Schlüssel drin, ändern Sie diesen in einen von Ihnen gewählten Schlüssel ab. Speichern Sie Ihre Eingabe durch anklicken des Buttons am Seitenende.

Diesen Schlüssel können Sie an die Nutzer herausgeben. Denken Sie bitte daran, dass Sie sich Namen und Ausweisnummer notieren und die Erklärung unterschreiben lassen!

Aktivieren Sie nun den URL-Filter für jugendgefährdende Seiten (BPjM-Modul).

FRITZ! **FRITZ!Box 7360**

FRITZ!Box | FRITZ!NAS | MyFRITZ!

Übersicht
Internet
Online-Monitor
Zugangsdaten
Filter
Freigaben
MyFRITZ!
DSL-Informationen
Telefonie
Heimnetz
WLAN
DECT
Diagnose
System

Filter

Kindersicherung | **Zugangsprofile** | Priorisierung | Listen

Mithilfe der Zugangsprofile legen Sie fest, wie die Netzwerkgeräte das Internet nutzen dürfen. Einige Profile sind bereits angelegt. Bei Bedarf können Sie diese bearbeiten und weitere Profile hinzufügen.

Name	Onlinezeit	Geteiltes Budget	Filter	Gesperrte Anwendungen		
Standard	unbegrenzt	—	—	—		
Gast	unbegrenzt	—	—	eMule, BitTorrent		
Unbeschränkt	unbegrenzt	—	—	—		
Gesperrt	keine	—	—	—		

Neues Zugangsprofil

Klicken Sie hier um das Gastprofil zu bearbeiten.



Übersicht

Internet

Online-Monitor
Zugangsdaten

Filter

Freigaben
MyFRITZ!
DSL-Informationen

Telefonie

Heimnetz

WLAN

DECT

Diagnose

System

Zugangsprofil Gast bearbeiten

Alle Netzwerkgeräte, die sich am FRITZ!Box-Gastnetz anmelden, bekommen automatisch das Zugangsprofil "Gast" zugewiesen. Richten Sie dieses Zugangsprofil hier Ihren Bedürfnissen entsprechend ein.

Name

Die Liste der Netzwerkgeräte, die dieses Profil nutzen, finden Sie unten im Bereich "Zugeordnete Netzwerkgeräte".

Zeitbeschränkung

Hier können Sie festlegen, innerhalb welchen Zeitraums die zugeordneten Netzwerkgeräte das Internet nutzen dürfen.

Zeitraum

immer
 nie
 eingeschränkt

0 2 4 6 8 10 12 14 16 18 20 22 24

Mo
Di
Mi
Do
Fr
Sa
So

0 2 4 6 8 10 12 14 16 18 20 22 24

■ Internetnutzung erlaubt
□ Internetnutzung gesperrt

Klicken Sie die Box zum Aktivieren des Filter.

Klicken Sie die Box zum Aktivieren des BPjM-Moduls.

Speichern Sie Ihre Eingabe.

Filter für Internetseiten

Legen Sie hier fest, ob für dieses Zugangsprofil Internetseiten gefiltert werden sollen und welche Liste verwendet werden soll.

- Internetseiten filtern
- HTTPS-Abfragen erlauben
- HTTPS wird beispielsweise für die Nutzung von Facebook, Gmail und Online-Banking verwendet. Beachten Sie bitte, dass diese Option alle Aufrufe über das Protokoll HTTPS erlaubt! Das gilt auch dann, wenn die aufgerufene Seite in einer angewendeten Filterliste enthalten ist.

Filterlisten

- Internetseiten erlauben (Whitelist) [\(Liste anzeigen\)](#)
- Nur die Internetadressen, die in der Whitelist enthalten sind, können aufgerufen werden.
- Internetseiten sperren (Blacklist) [\(Liste anzeigen\)](#)
- Alle Internetadressen, die in der Blacklist enthalten sind, sind gesperrt. Aufrufe über IP-Adressen sind ebenfalls gesperrt. [\(Ausnahmen anzeigen\)](#)

- jugendgefährdende Internetseiten sperren (BPjM-Modul)
- Zusätzlich werden die von der BPjM indizierten Internetseiten gefiltert.

Hinweis:

Die Filterlisten Whitelist und Blacklist können Sie im Bereich Internet/Filter/Listen lesen und bearbeiten.

German - Wichtige Hinweise zur Nutzung des Internetanschlusses

Mit dem Erhalt der Zugangsdaten können Sie den Internetanschluss nutzen. Bitte beachten Sie dass der Internetanschluss Ihnen von Dritten zur Verfügung gestellt wird. Der Anschlussinhaber ist eine Privatperson bzw. ein privater Verein.

Sie verpflichten sich nachfolgende Regeln zu beachten:

Es ist Ihnen nicht erlaubt die Zugangsdaten weiterzugeben. Die Nutzung des Anschlusses ist nur durch Sie persönlich gestattet!

Sie unterliegen den gesetzlichen Bestimmungen zur Internetnutzung in Deutschland. Der Betreiber kann Ihre Verbindungsdaten speichern und wird Sie beim Verdacht einer Straftat den Behörden zur Verfügung stellen.

Insbesondere ist folgendes nicht erlaubt:

- Der Aufruf zu Straftaten über das Internet.
- Die Organisation von Straftaten über das Internet
- Das Veröffentlichen von diffamierenden, beleidigenden oder hetzerischen Inhalten
- Das unberechtigte Herunterladen und/oder weitergeben von urheberrechtlich geschützten Daten wie zum Beispiel Filme, Musik oder Computerspielen
- Das Einschleusen von Computerviren oder Schad-Software
- Die Nutzung von Webseiten mit pornografischem Inhalt
- Die Verbreitung von pornografischen Inhalten

Darüber hinaus gelten die gesetzlichen Bestimmungen.

Durch Ihre Unterschrift erkennen Sie die oben genannten Bedingungen an.

.....

Datum, Unterschrift

English - Important notes on using the Internet connection

By receiving the login information, you can use the Internet. Please note that the internet is brought to you by third parties. The connection owner is an individual or a private association.

You agree to observe the following rules:

Do not pass the login information to anybody. The use of the connection is only permitted by you personally!

The usage is subject to the statutory provisions for Internet use in Germany. The operator can save your connection information and make it available to the authorities when a crime is suspected.

In particular, the following are not allowed:

- The call for criminal offenses on the Internet.
- The organization of crime on the Internet
- The publication of defamatory, abusive or hateful content
- Unauthorized downloading and / or sharing copyrighted data such as movies, music or video games
- The distribution of computer viruses or harmful software
- The use of websites with pornographic content
- The distribution of pornography

In addition, the statutory provisions for Internet use in Germany apply.

By signing below, you agree to the above terms and conditions.

.....
Date, Signature

French/Français - Remarques importantes sur l'utilisation de la connexion Internet

En recevant les informations de connexion, vous pouvez utiliser l'Internet. S'il vous plaît, notez que l'Internet vous est présenté par des tiers. Le propriétaire de la connexion est une personne ou une association privée.

Vous vous engagez à respecter les règles suivantes:

Vous ne pouvez pas partager les informations de connexion à personne. L'utilisation de la connexion n'est autorisée qu'à vous!

L'utilisation de l'Internet est soumise aux dispositions légales relatives à l'utilisation d'Internet en Allemagne. L'opérateur peut enregistrer vos informations de connexion et les mettre à la disposition des autorités quand un crime est soupçonné.

En particulier, les éléments suivants ne sont pas admis:

- L'appel pour des infractions pénales sur Internet.
- L'organisation de crimes sur Internet
- La publication de contenus diffamatoires, offensants ou haineux
- Téléchargement et / ou le partage non-autorisé de données protégées comme films, musique et jeux vidéo
- La distribution de virus informatiques ou de logiciels malveillants
- L'utilisation de sites Web à contenu pornographique
- La propagation de la pornographie

En outre, les dispositions légales relatives à l'utilisation d'Internet en Allemagne s'appliquent.

En signant ci-dessous, vous acceptez les termes et conditions ci-dessus.

.....
Date, Signature

Arabic/عربي - ملاحظات هامة حول استخدام خدمة الإنترنت

من خلال تلقّي معلومات تسجيل الدخول، يمكنك استخدام الإنترنت. يرجى الملاحظة أن الإنترنت تقدمه من قبل طرف ثالث. صاحب الخدمة فرد أو شركة خاصة.

أنت توافق على الالتزام بالقواعد التالية:

لا تستطيع تمرير معلومات تسجيل الدخول الى أحد. يسمح فقط لك باستخدام الانترنت!

يخضع الاستخدام للأحكام القانونية على استخدام الإنترنت في ألمانيا. يمكن للمشغل توفير معلومات الاتصال الخاصة بك للسلطات عند الاشتباه بجريمة.

على وجه الخصوص، لا يسمح فيما يلي:

- الدعوة لجرائم جنائية على شبكة الإنترنت
 - تنظيم جريمة على شبكة الإنترنت
 - نشر محتويات تشهيرية، مسيئة أو حاقة
 - تحميل أو تبادل البيانات الغير مصرحة بها وفقاً لحقوق الطبع والنشر مثل الأفلام و الموسيقى و ألعاب الفيديو
 - نشر فيروسات الكمبيوتر أو البرامج الضارة
 - استخدام المواقع الإباحية
 - نشر المواد الإباحية
- إضافةً إلى ما تنص عليه الأحكام القانونية على استخدام الإنترنت في ألمانيا.

من خلال التوقيع أدناه، فإنك توافق على الشروط الواردة أعلاه.

.....
التوقيع، التاريخ

Italian - Note importanti sul usando la connessione a Internet

Ricevendo le informazioni di accesso, è possibile utilizzare Internet. Si prega di notare che internet è portato a voi da parte di terzi. Il proprietario di collegamento è un individuo o di un associazione privato.

L'utente accetta di rispettare le seguenti regole:

Non si può permettere il pass di accesso. L'uso della connessione è consentita solo da personale! Essi sono soggetti alle disposizioni di legge in materia di uso di Internet in Germania. L'operatore può salvare le informazioni di connessione e mettere a disposizione delle autorità quando si sospetta un crimine.

In particolare, non sono ammessi i seguenti:

- La richiesta di reati su Internet.
- L'organizzazione della criminalità su Internet
- La pubblicazione di contenuti diffamatori, offensivi o odioso
- Download e / o condivisione non autorizzata di dati protetti da copyright, come film, musica o videogiochi
- Il contrabbando di virus informatici o software dannoso
- L'uso di siti web con contenuti pornografici
- La diffusione della pornografia

Inoltre, le disposizioni di legge.

Con la firma di seguito, l'utente accetta i termini e le condizioni di cui sopra.

.....
Data, Firma

Somali - Qoraallo muhiim ah oo ku saabsan isticmaalaya internet ku

By helaya war login, waxaad isticmaali kartaa Internetka. Fadlan la soco in internet ka waxaa kuu keenay qaybaha sadexaad. Milkiilaha xiriir waa qof ama koox gaar ah.

Waxaad ogolaatay inay dhawraan xeerarka soo socda:

Waxaad ma oggolaan karaan pass ay helaan. Icticmaalka xiriir la ogol yahay oo keliya in aad shakhsi! Waxay hoos imaanaysa qodobada sharciga ahi ku leeyihiin isticmaalka Internet ee Germany yihiin. Operator waxa uu badbaadin karaa macluumaad la xiriira, waxayna diyaar u ah masuuliyiinta marka fal dambi ah lagu tuhunsan yahay.

Gaar ahaan, waxa soo socda aan la ogolaan:

- Call ee fal-dembiyeed ee internetka.
- Ururka ayaa ah dambiyada internetka ee
- Qoraalkan wuxuu ka kooban ceebayn, xadgudub ama lagu Neceb yahay
- Dajinta oggoleyn iyo / ama wadaagista xogta xuquuqdiisa sida filimada, muusikada ama kulan video
- Tahriibinta ayaa ka mid ah fayrasyada computer ama software waxyeello
- Icticmaalka boggaga waxyaabaha websedyada
- Faafidda filimada

Intaa waxaa dheer, qodobada sharci ah.

Saxeexa hoosta, aad ogolaato inaad shuruudaha iyo xaaladaha kor ku xusan.

.....
Date, Saxiixa

انٹرنیٹ کنکشن کا استعمال کرتے ہوئے پر اہم نوٹس
لاگ ان معلومات کو حاصل کر کے، آپ انٹرنیٹ استعمال کر سکتے ہیں۔ انٹرنیٹ تیسری پارٹیوں کی طرف سے آپ
کے لئے لایا جاتا ہے براہ مہربانی نوٹ کریں۔ کنکشن کے مالک کو ایک فرد یا ایک نجی کلب ہے۔
آپ کو مندرجہ ذیل قوانین پر عمل کرنے سے اتفاق:
آپ رسائی پاس اجازت نہیں کر سکتے۔ کنکشن کے استعمال کو صرف ذاتی طور پر آپ کی طرف سے کی اجازت
ہے!
وہ جرمنی میں انٹرنیٹ کے استعمال پر قانونی دفعات کے ساتھ مشروط ہیں۔ آپریٹر آپ کے کنکشن کی معلومات کو
بچانے کے اور ایک جرم شبہ ہے جب حکام کو دستیاب کر سکتے ہیں۔
خاص طور پر، مندرجہ ذیل کی اجازت نہیں ہے:
- انٹرنیٹ پر فوجداری جرائم کے لئے کال۔
- انٹرنیٹ پر جرائم کی تنظیم
-، آمیز توہین آمیز یا نفرت مواد کی اشاعت
- ایسی فلموں، موسیقی یا ویڈیو گیمز کے طور پر غیر مجاز ڈاؤن لوڈ کرنے اور / یا شیئرنگ کاپی رائٹ ڈیٹا
- کمپیوٹر وائرس یا نقصان دہ سافٹ ویئر کی سمگلنگ
- فحش مواد کے ساتھ ویب سائٹس کے استعمال
- فحاشی کو پھیلانے سے
اس کے علاوہ، قانونی دفعات۔
ذیل میں دستخط کر کے، آپ کے اوپر شرائط و ضوابط سے اتفاق کرتا ہوں۔

.....
تاریخ، دستخط

Urdu

Yoruba - Pataki awon akosile lori lilo isopo Ayelujara

Nipa gbigba awon alaye wiwole re, o le lo Ayelujara. Jowo se akiyesi pe ayelujara wa ni mu si o nipa awon eni keta. Awon asopo eni je eya kookan tabi a ikoko Ologba.

O ti gba lati ma kiyesi awon wonyi ofin:

O le ko gba laaye wiwole koja. Awon lilo ti awon asopo ti wa ni nikan yoda nipase o tikalarare!
Won ti wa ni koko si amofin ipese lori ayelujara ti lilo ni Germany. Awon onise le fi re asopo alaye ati ki o se wa si awon alase nigbati a odaran ti wa ni fura si.

Ni pato, awon wonyi ni a ko gba laaye:

- Awon ipe fun odaran ese lori ayelujara.
- Awon agbari ti odaran lori ayelujara
- Awon atejade ti defamatory, meedogbon tabi korira akoonu
- Laigba downloading ati / tabi nipa sise aladako data gegebi sinima, awon ere orin tabi fidio
- Awon smuggling ti komputa virus tabi ipalara software
- Awon lilo ti awon aaye ayelujara pelu pornographic akoonu
- Awon itankale ti aworan iwokuwo

Ni afikun, awon amofin ipese.

Nipa wiwole si isale, ti o ti gba si awon loke ofin ati ipo.

.....
Ojo, Ibuwole

Sudanese - Catetan penting make sambungan Internet

Ku narima informasi login, Anjeun bisa maké Internét. Punten dicatet yén internet ieu dibawa ka anjeun ku pihak katilu. Nu boga sambungan nyaéta hiji individu atawa klub swasta.

Anjeun satuju pikeun niténan aturan di handap ieu:

Anjeun teu bisa ngidinan aksés lulus. Pamakéan sambungan ngan diijinkeun ku Anjeun pribadi! Maranehna nunut ka dibekelan statutory dina pamakéan Internét di Jerman. Operator bisa nyimpen informasi sambungan anjeun sarta nyieun sadia ka otoritas lamun kajahatan hiji disangka.

Dina sababaraha hal, di handap ieu teu diidinan:

- Telepon nu keur nyinggung kriminal dina internét.
- Nu organisasi kajahatan di Internét
- Nu publikasi eusi fitnah, kasar atawa hateful
- Teu diidinan diundeur jeung / atawa babagi data nu gaduh hak cipta saperti pilem, musik atawa video games
- Nu nyalurkeun virus komputer atawa software ngabahayakeun
- Pamakéan situs web jeung eusi porno
- Sumebarna pornografi

Sajaba ti éta, nu dibekelan statutory.

Ku Signing di handap, Anjeun satuju istilah jeung kaayaan di luhur.

.....
Tanggal, tekenan

Krio - Wetin u for dae memba ol tem wae yu dae use di intanet

Wae u get di login informashon, u kin ebl use di intanet. Duya mek yu know say di intanet dae kam tu yu from oda pati dem. Di wan dem wae get am kin bi sombodi or oda pipul dem wae kam togeda.

Yu don gree for folow den rul ya:

Duya nor gee nobodi yu login informashon. Memba say na yu nomor get rite for use am!

Law dae na Germany wae dae chek haw for use di intanet. Di wan wae na e nomor get rite panam kin tek tem kip anytin en show am to govment mor if e get somtin wae nor gud at al for di kontri.

Den wanya so mor, den nor dae gree pan dem at al at al:

- Wae dae use di intanet fo cal pipul dem pa bad.
- Wae yu dae use di intanet for bring pipul dem togeda for do bad.
- Wae yu dae mek den bad bad tok, yu dae use den bad wod or somtin wae go mek pipul dem hate demsef.
- Wae yu dae get somtin na di intanet wae yu nor get rite pa en / or wae yu dae shabe tin dem lek dem movi, msik, or dem vidio game.
- Wae yu dae skata den komputa sik or den bad tin wae go powel di komputa.
- Wae yu dae put den rude tin dem na di website.
- Wae yu dae skata den rude rude tin dem.

For saka dis, di law dem na Germany don lef yu wae dae use di intanet.

As yu dae rite yu nem na ya so, dat don show say yu don gree wit al wetin bin dae pantap dis paypa ya so.

.....
Di date en yu nem.

Shënime të rëndësishme për përdorimin e qasjes në Internet

Duke marrë login informacion ju mund të përdorni internetin. Ju lutem vini re se lidhja e internetit do të ofrohet nga palët e treta. Mbajtësi lidhës është një person privat apo një shoqatë private. Ju pranoni të respektojë rregullat e mëposhtme: Kjo nuk ju lejon të kalojë në të dhënat e hyrjes. Përdorimi i lidhjes është i lejuar vetëm nga ju personalisht!

Ata janë subjekt i rregullativës ligjore mbi përdorimin e internetit në Gjermani. Operatori mund të ruajë të dhënat tuaja lidhjes dhe do të vërë në dispozicion të autoriteteve kur një krim është i dyshuar.

Në veçanti, në vijim nuk është e lejuar:

- Thirrja për vepra penale në internet.
- Organizimi i krimit në Internet
- Botime shpifëse, përmbajtje fyese ose të urrejtëshme
- Shkarkimit paautorizuar dhe / ose ndarjen e të dhënave copyright tilla si filma, muzikë apo lojra kompjuterike
- Kontrabanda e viruseve kompjuterike ose software qëllim të keq
- Përdorimi i faqeve me përmbajtje pornografike
- Përhapja e pornografisë Për më tepër, dispozitat ligjore.

Duke nënshkruar më poshtë, ju pranoni kushtet e mësipërme.

.....

Data, Nënshkrimi



د اینټرنټ د استفادې کولو قرارداد

پښتو

چې وروسته د دې نه چې تاسو کانت شولی تاسو کولای شئ چې کله واخلئ

دا لارښوې چې تاسو په دې باندې پوره وی چې دغه اینټرنټ د بل چا په نوم دی او

هغه دا حق لري چې د دې اینټرنټ د استعمال کول طریقې وټاکي او تاسو مني چې لاندې قوانین مراعات کوی:

۱- تاسو دا حق نلری چې دغه کوډ چې تاسو ته ورکړ شوی ده بل چا ته ورکړئ (وکړئ)

۲- د دې کوډ د استفادې کول یوازې تاسو لپاره دی.

۳- هغه قوانین چې په آلمانی خلک د اینټرنټ د استفادې کول دی په تاسو باندې هم دی.

۴- او تاسو دا هم مني چې د تاسو ټول ځانګړتیا (اسم) دلته ثبت کیږي او که د تاسو نه کوم استفساره سوږه مشاهده وشو او هغه مطلبونه چې تاسو حق نلری چې پست وکړئ او که چاته ولیږي تاسو په محکمه لېږل کیږي.

- د دې مطلبونه د استفادې کول منع دی:

۱- د جرم د اجرا کولو لپاره خلک د محبت کول

۲- هغه ګروپونو جوړول چې د جرم لپاره وی

۳- توهین کول، حمله کول او ځینې مضر ټیم او فیلمونو اینټرنال کول او دانلود کول.

۴- هغه مطلبونو داخلول چې مضر وی لکه: وایرس او د خلکو وسایل متوقف کول

۵- د هغه پروګرامونه استفادې کول چې مضر دی.

۶- او هغه (هغه) پروګرامونو داخل کول چې مضر وی (مضر عشقی)

Tigrinya

መእተዊ ምስተዋሃብኩም ኢንተርነት ክትኣትዉ ትኽእሉ ኢኹም።

በጃኩም ግን እዚ ዝመጸኩም ዝሎ ካብ ሳልሳይ ኣካል እዩ።እዚ ናይ ሓደ ጥርኑ እዩ።

በዘን ሕግታት ክትጥቀሙ ኣወ በሉ ነዚ ታስዎርድ ንዝኮነ ሰብ ኣይትሃብዎ መኻንያቱ ምጥቃም ናይዚ ኢንተርነት ኮኔክሽን ንዓኻ ጥራይ ኣዩ ዝምልከት።

ኣዚፈነወ ብሕጊ ጀርመን ኣዩ ዝከይድ።እዚ ኢንተርነት ትርዝግሉ ካም ኒ ብዝኮነ ገበን ምስ ትገብር ኣብ ሕጊ ከረካክቡልካ ይኽእሉ እዮም።

ዘይ ቐቡላት ተግባራት (ሕግታት)

- ※ ኣብ ኢንተርነት ገበናት ምድዋል ኣይ ቀድን ኣዩ።
- ※ ምስ ሰብ ገበናት ምትሕብባር ኣይ ቀድን ኣዩ።
- ※ ዝኮነ ናይ ጽልኢ ሕጻን ተግባራት ምስዳድ ወይ ምዝርጋሕ ኣይ ቀድን።
- ※ ብዘይ ሕጊ ሙዚቃ፡ቪድዮ፡ጌም ምውራድ ኣይ ቀድን እዩ።
- ※ ምዝርጋሕ ሻይረስ ናይ ኮም ተር ወይ ድማ ሮግራም ኣይ ቀድን።
- ※ ምጥቃም ሴክስ ወብሳይት ኣይ ከድን።
- ※ ምዝርጋሕ ሴክስ ወብሳይት ውን ኣይ ከድን።

ብዝያዳ ሕጊ ኢንተርነት ናይ ጀርመን ተግባራዊ ኣዩ።

ኣብ ታሕቲ ኣንድሕር ፈሪምካ ነቲ ኣብ ላዕሊ ዝተጻሕፈ ተከቢላዮ ኣለኩ ማለት ኣዩ።

Немецкий язык — Важные указания по пользованию Интернетом

Получив данные для доступа, вы можете пользоваться Интернетом. Просьба обратить внимание на то, что подключение к Интернету в ваше распоряжение предоставляется третьим лицом. Владелец Интернет-присоединения является частное лицо или частное общество.

Вы обязуетесь соблюдать нижеследующие правила:

Вам не разрешается передавать третьим лицам данные для доступа в Интернет. Пользоваться Интернетом разрешается исключительно лично вам!

В Германии вы обязаны соблюдать предписанные законом правила пользования Интернетом. Оператор может сохранять ваши параметры соединения и предоставит их соответствующим органам при подозрении на совершение наказуемых действий.

В частности, запрещены ниже перечисленные пункты:

- призыв к совершению преступлений посредством интернета;
- организация преступлений посредством интернета;
- опубликование содержаний, содержащих клевету, оскорбления или подстрекание;
- незаконное скачивание и/или передача третьим лицам таких данных, охраняющихся авторским правом, как например, фильмы, музыка или компьютерные игры;
- внедрение компьютерного вируса или вредоносных программ;
- использование Интернет-сайтов с порнографическим содержанием;
- распространение порнографического содержания.

Кроме того, действуют законные предписания.

Подписывая этот документ, вы соглашаетесь с вышеназванными условиями.

.....

дата, подпись

Beispiel-Voucher – Nicht gültig

Serial Number: Roll 200 Nr. 445

Vouchercode:

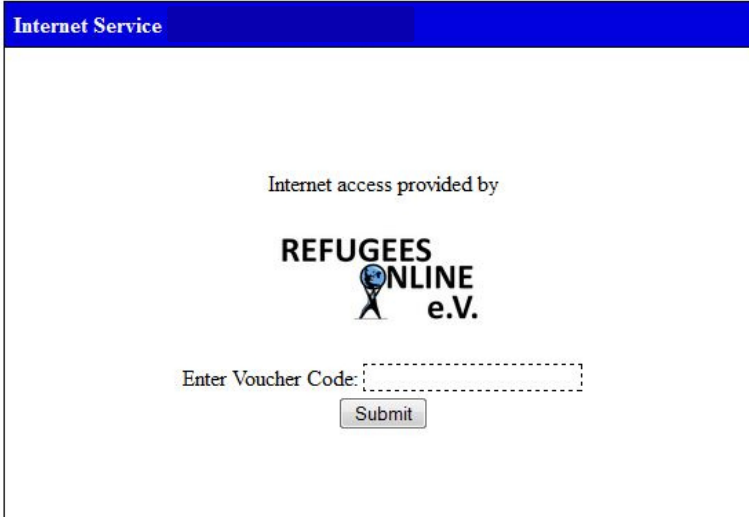
YsdmMzKAqPS



Your Internet Voucher

Instructions:

- Connect your device to WiFi „RefugeesOnline“
- Open your browser
- Type in: **www.refugees-online.de**
- The following page shows up:



The screenshot shows a web page titled "Internet Service" with a blue header. The main content area contains the text "Internet access provided by" followed by the "REFUGEES ONLINE e.V." logo. Below the logo, there is a text input field labeled "Enter Voucher Code:" and a "Submit" button.

- Type your voucher code into the field, the code is case-sensitive!
- Click on „Submit“
- Your internet connection is established
-

Please note:

- You will be automatically logged out after 15 minutes of inactivity
- If that happens, re-enter your voucher code and click „Submit“
- You will be automatically logged out after two hours for security reasons
- If that happens, re-enter your voucher code and click „Submit“
- Your voucher code expires after 30 days. Come back and get a new one.
-

Do not give your code to someone else! You will not be able to use the service anymore if your code is used by someone else!

You can use the voucher code for different devices, but only one at a time!
Avoid congestion. The Internet line is shared with others and the service may not work properly if too many people are logged in at the same time.
Always remember: Traffic will be logged by the provider. You are fully responsible for any misuse. **Violators of the German law will be prosecuted!**

In case of problems write an email to support@refugees-online.de