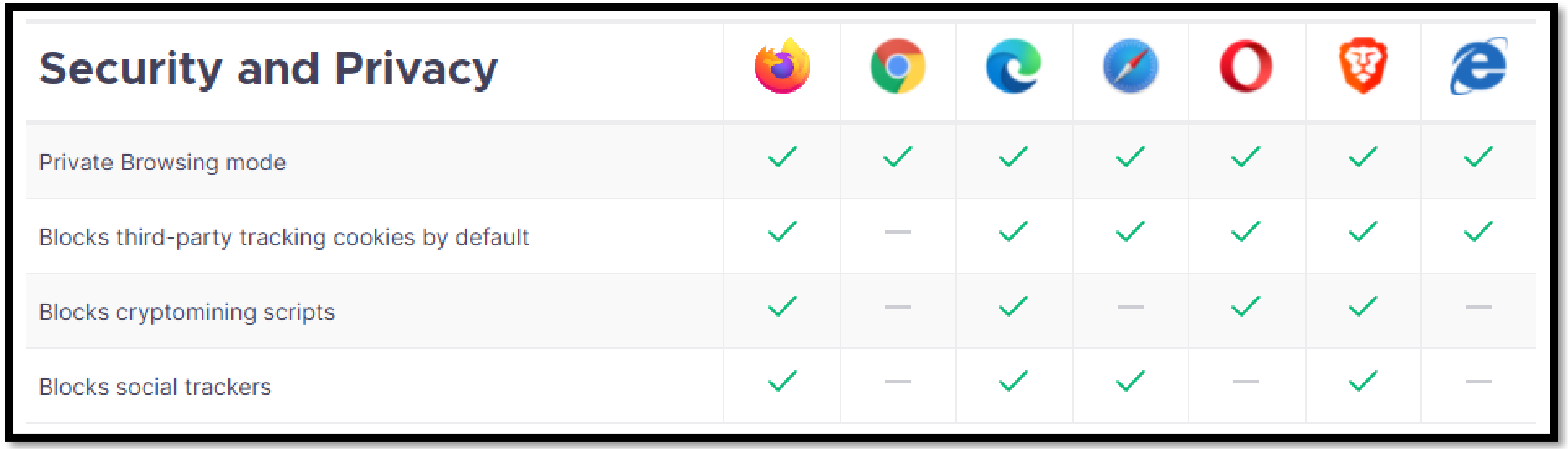
Are you ready? II

S1 Personal Security

D4 – Data and Ethics // Coaching

Individual Protection

Smartphone / Desktop



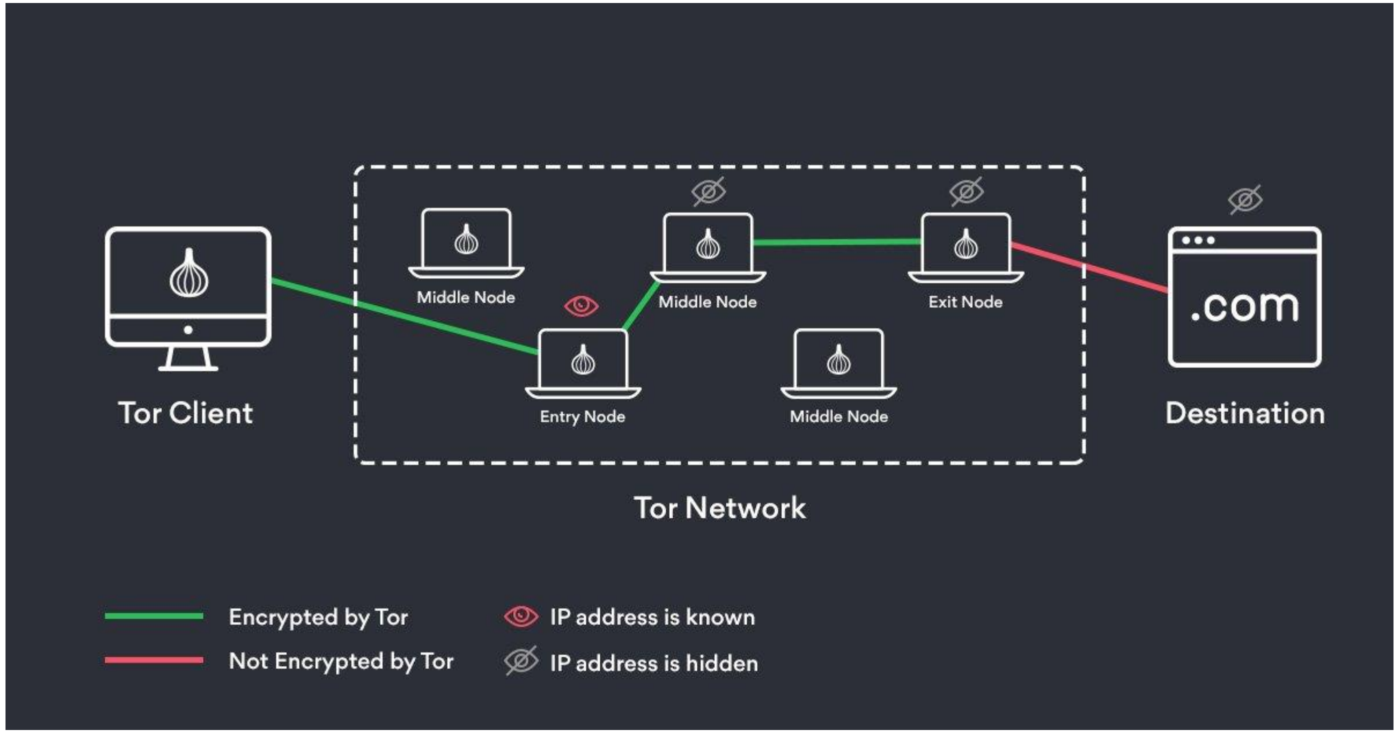
Security and Privacy							
Private Browsing mode	✓	✓	✓	✓	✓	✓	✓
Blocks third-party tracking cookies by default	✓	—	✓	✓	✓	✓	✓
Blocks cryptomining scripts	✓	—	✓	—	✓	✓	—
Blocks social trackers	✓	—	✓	✓	—	✓	—

https://www.mozilla.org/en-US/firefox/browsers/compare/

Individual Protection

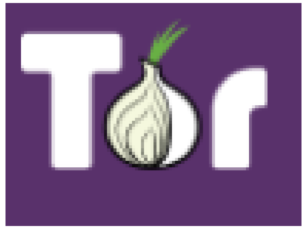
Smartphone / Desktop

other Browser - TOR



Verteidige dich.

Schütze dich vor Verfolgung, Überwachung und Zensur.



https://3g2upl4pq6kufc4m.onion

TOR - DuckDuckGo

https://www.torproject.org/de/download/

Individual Protection

Smartphone / Desktop

Other Search Engine - DuckDuckGo

DuckDuckGo
Datenschutz – leicht gemacht. Hilf, DuckDuckGo zu verbreiten!

https://proprivacy.com/blog/duckduckgo-safe

Is DuckDuckGo safe?

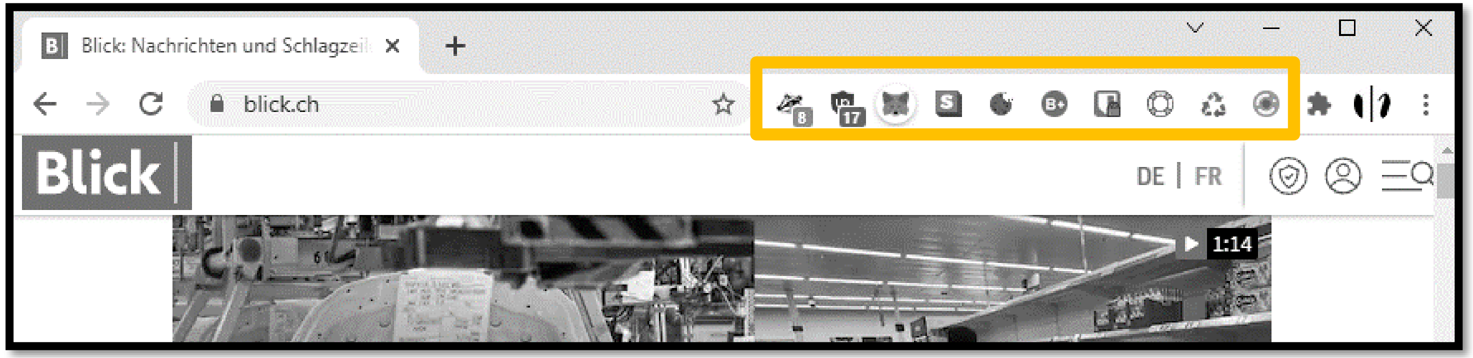
When you use Google, Bing or any other popular search engine, data about your browsing habits is sent to the site you clicked on when you click on links. Information such as your IP address is also sent to the site. DuckDuckGo, on the other hand, does not send the terms you type into the search engine or your browsing activity to the sites you search for. A website may know that you clicked on a link, but it doesn't learn how you got to that link or what else you searched for.

Browser-Extensions

Individual Protection

Smartphone / Desktop

Browser-Extensions (Add-Ins, Add-Ons, Plugins, Erweiterungen)



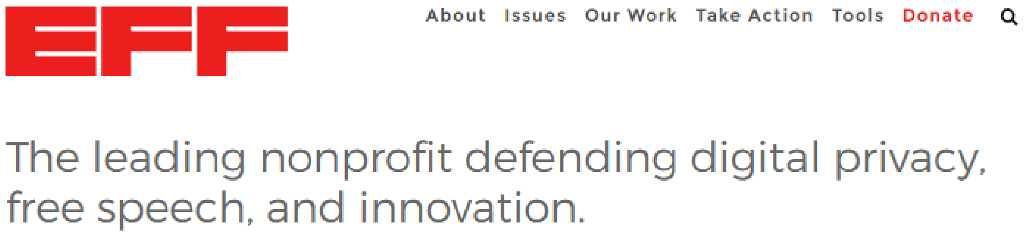
Browser-Extensions

Individual Protection

Smartphone / Desktop

What is Privacy Badger?

Privacy Badger is a browser add-on that stops advertisers and other third parties from secretly tracking where you go and what pages you view on the Internet. If an advertiser tracks you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading more content in your browser. For the advertiser, it's as if you suddenly disappeared.



The leading nonprofit defending digital privacy, free speech, and innovation.

https://privacybadger.org/

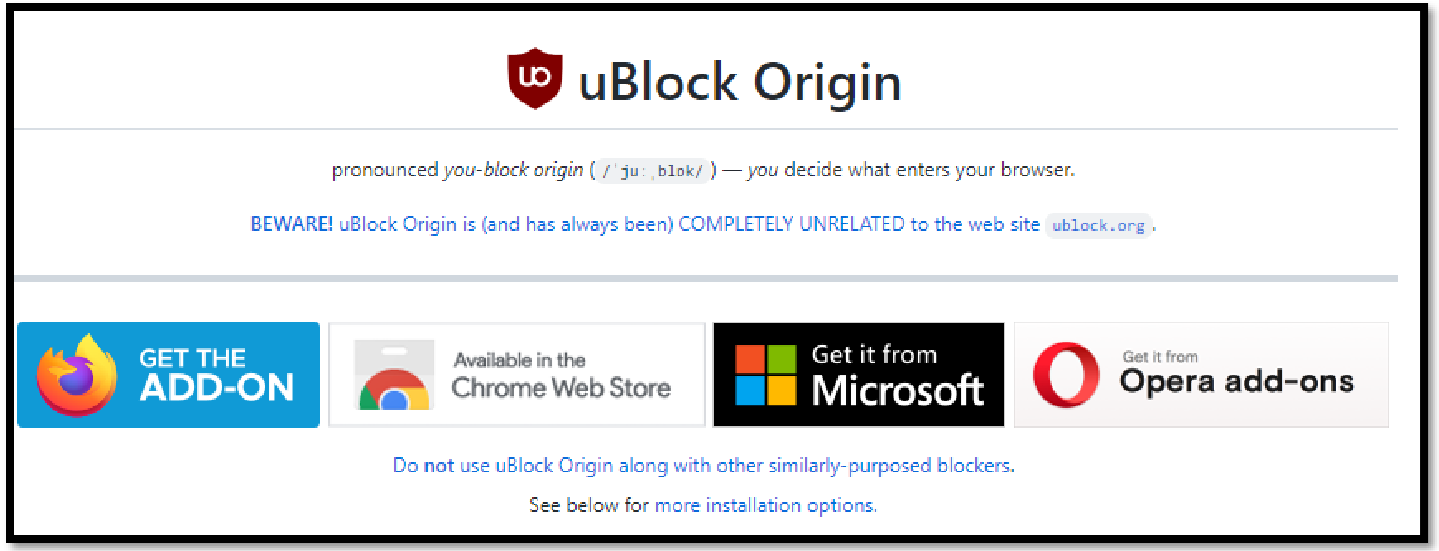
Browser-Extensions

Individual Protection

Smartphone / Desktop

What is uBlock Origin?

uBlock Origin is NOT an "ad blocker": it is a broadband blocker that happens to be able to function as a pure "ad blocker" as well. When uBlock Origin is reinstalled, it blocks ads, trackers and malware sites by default - via EasyList, EasyPrivacy, Peter Lowe's ad/tracking/malware server, Online Malicious URL Blocklist and uBlock Origin's own filter lists.



uBlock Origin

pronounced *you-block origin* (/ˈjuː ˌblɒk/) — *you* decide what enters your browser.

BEWARE! uBlock Origin is (and has always been) COMPLETELY UNRELATED to the web site ublock.org.

Do not use uBlock Origin along with other similarly-purposed blockers.

See below for more installation options.

https://github.com/gorhill/uBlock/wiki

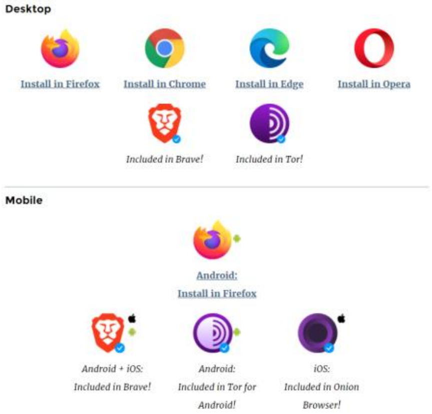
Browser-Extensions

Individual Protection

Smartphone / Desktop

What is HTTPS://EVERYWHERE?

HTTPS Everywhere is being developed in collaboration between the Tor Project and the Electronic Frontier Foundation. Many websites offer limited support for encryption over HTTPS, but make it difficult to use. For example, they may use unencrypted HTTP or populate encrypted pages with links that link back to the unencrypted page. The HTTPS Everywhere extension fixes these problems by using smart technology to rewrite requests to these websites to HTTPS.



https://www.eff.org/https-everywhere

Browser-Extensions

Individual Protection

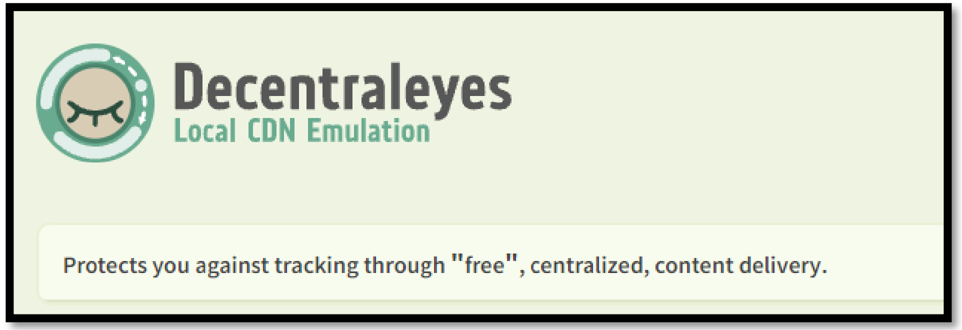
Smartphone / Desktop

What is Decentraleyes?

The increasing prevalence of third-party scripts embedded in websites allows user tracking by the provider of the script, who thus gains insight into which user accessed which page and when. If the user does not want to provide this information to protect his privacy, he can use an ad blocker to prevent such scripts from loading. In most cases, the user then experiences that the page does not function properly without the scripts or does not display any content at all. The Decentraleyes browser extension makes it possible to display the content of pages correctly without revealing personal data to a third party (script provider). It should be seen as a complement to existing ad blockers such as uBlock Origin or Adblock Plus.

How it works

In simple terms, the extension prevents access to the respective external service initiated by Internet pages for frequently encountered libraries and instead makes them available locally on the user's computer. Thus, the external service no longer receives information about which Internet pages have been accessed from a computer, and about which topics a user has read up on which pages.



Decentraleyes

Local CDN Emulation

Protects you against tracking through "free", centralized, content delivery.

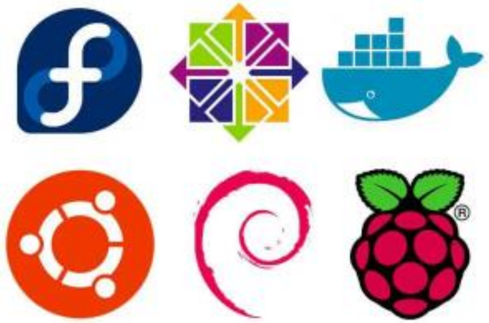
https://decentraleyes.org/

Individual Protection

Smartphone / Desktop

Pi-Hole

Pi-hole not only blocks advertisements, but also has an informative web interface that displays statistics about all domains that are queried on your network. Built-in DHCP server Pi-hole works well with an existing DHCP server, but you can use Pi-hole's to keep your network management in one place.



https://pi-hole.net/

Browser-Extensions

Individual Protection

Smartphone / Desktop

Firewall

A personal firewall (also known as a decentralized firewall or desktop firewall) is a software solution that is installed on the end devices. It is intended to protect against access from the network. It is also designed to prevent certain programs, such as spyware, from making contact with the Internet from the inside. Some personal firewalls also restrict the access of any program to system resources (so-called sandboxing). This is to allow a possibly unsafe program to be used without any major risks. Such functionality can be useful, for example, with browsers that run active content.

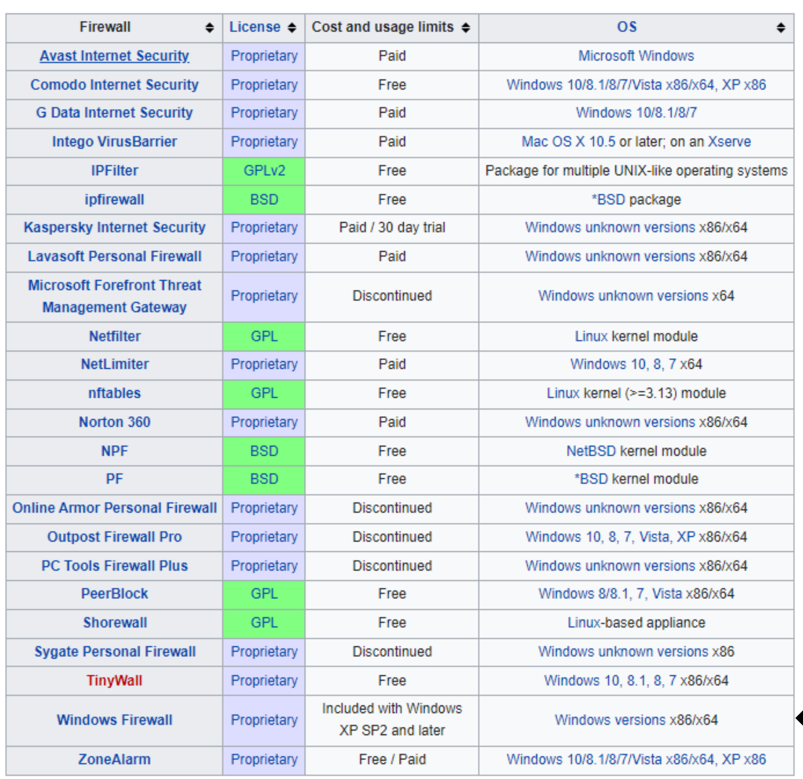
https://www.bsi.bund.de/DE/Service-Navi/FAQ/PersonalFirewall/faq_personalfw_node.html

Browser-Extensions

Individual Protection

Smartphone / Desktop

Firewall-Software



Firewall	License	Cost and usage limits	OS
Avast Internet Security	Proprietary	Paid	Microsoft Windows
Comodo Internet Security	Proprietary	Free	Windows 10/8.1/8/7/Vista x86/x64, XP x86
G Data Internet Security	Proprietary	Paid	Windows 10/8.1/8/7
Intego VirusBarrier	Proprietary	Paid	Mac OS X 10.5 or later; on an Xserve
IPFilter	GPLv2	Free	Package for multiple UNIX-like operating systems
ipfirewall	BSD	Free	*BSD package
Kaspersky Internet Security	Proprietary	Paid / 30 day trial	Windows unknown versions x86/x64
Lavasoft Personal Firewall	Proprietary	Paid	Windows unknown versions x86/x64
Microsoft Forefront Threat Management Gateway	Proprietary	Discontinued	Windows unknown versions x64
Netfilter	GPL	Free	Linux kernel module
NetLimiter	Proprietary	Paid	Windows 10, 8, 7 x64
nftables	GPL	Free	Linux kernel (>=3.13) module
Norton 360	Proprietary	Paid	Windows unknown versions x86/x64
NPF	BSD	Free	NetBSD kernel module
PF	BSD	Free	*BSD kernel module
Online Armor Personal Firewall	Proprietary	Discontinued	Windows unknown versions x86/x64
Outpost Firewall Pro	Proprietary	Discontinued	Windows 10, 8, 7, Vista, XP x86/x64
PC Tools Firewall Plus	Proprietary	Discontinued	Windows unknown versions x86/x64
PeerBlock	GPL	Free	Windows 8/8.1, 7, Vista x86/x64
Shorewall	GPL	Free	Linux-based appliance
Sygate Personal Firewall	Proprietary	Discontinued	Windows unknown versions x86
TinyWall	Proprietary	Free	Windows 10, 8.1, 8, 7 x86/x64
Windows Firewall	Proprietary	Included with Windows XP SP2 and later	Windows versions x86/x64
ZoneAlarm	Proprietary	Free / Paid	Windows 10/8.1/8/7/Vista x86/x64, XP x86

Microsoft Security Essentials has reached end of service on January 14, 2020 and is no longer available for download. Microsoft will continue to release signature updates (including Engine) for service systems currently running Microsoft Security Essentials until 2023.

Alternative:
Windwos Defender - Next generation protection against viruses and malware. Tracking prevention.2 ~~Biometric logins~~.3 All integrated, always updated, and at no additional cost to you.7

https://en.wikipedia.org/wiki/Comparison_of_firewalls

https://www.microsoft.com/en-us/download/details.aspx?id=54795

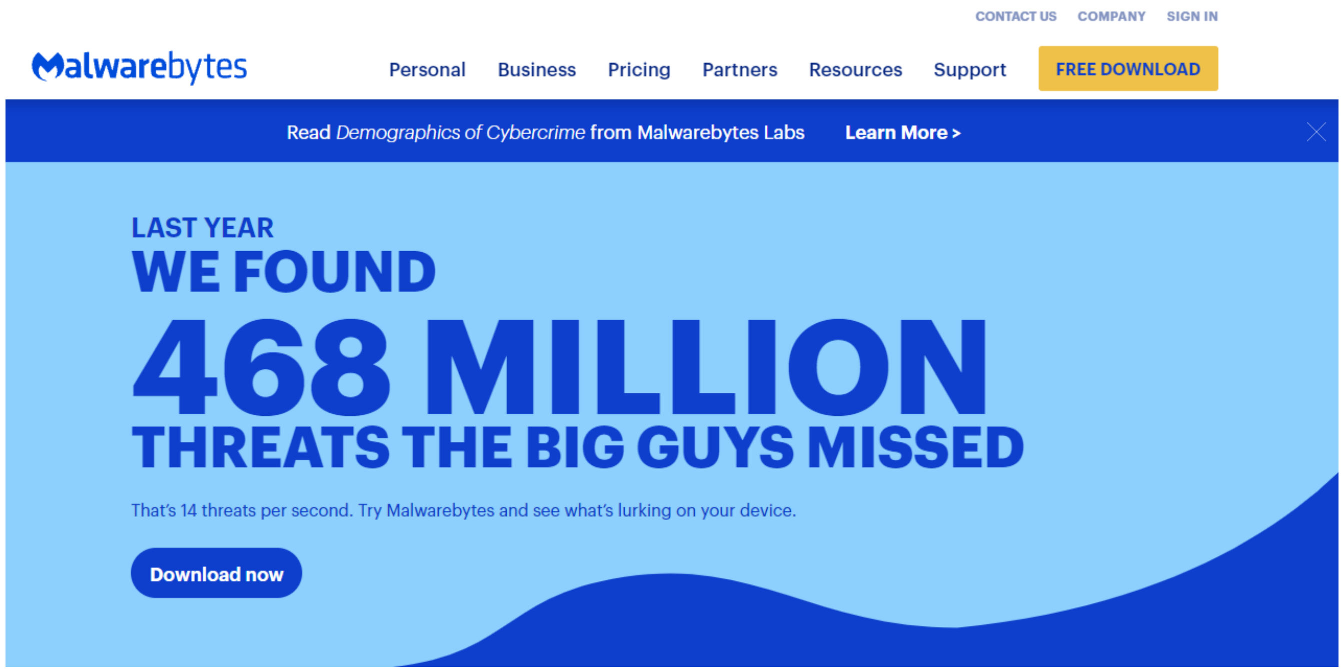
Browser-Extensions

Individual Protection

Smartphone / Desktop

Firewall-Software

https://www.malwarebytes.com/



CONTACT US COMPANY SIGN IN

Malwarebytes Personal Business Pricing Partners Resources Support FREE DOWNLOAD

Read *Demographics of Cybercrime* from Malwarebytes Labs Learn More >

LAST YEAR
WE FOUND
468 MILLION
THREATS THE BIG GUYS MISSED

That's 14 threats per second. Try Malwarebytes and see what's lurking on your device.

Download now

https://www.trojaner-board.de/

RogueKiller
Anti Malware
The next generation virus scanner. Find unknown malware, stay protected.

https://www.adlice.com/roguekiller/#alt_download

University of Applied Sciences and Arts Northwestern Switzerland
School of Life Sciences

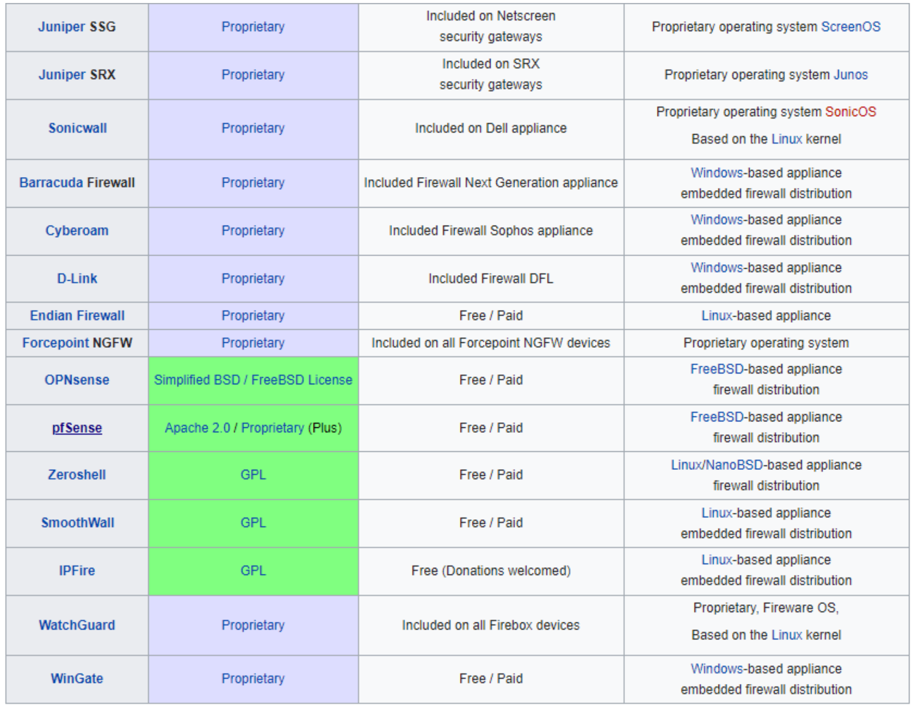
Browser-Extensions

Individual Protection

Smartphone / Desktop

Firewall-Appliances

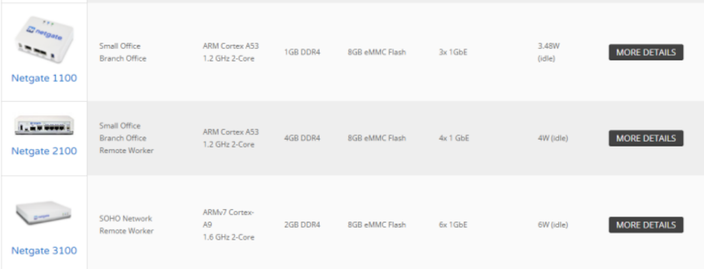
https://en.wikipedia.org/wiki/Comparison_of_firewalls



Juniper SSG	Proprietary	Included on Netscreen security gateways	Proprietary operating system ScreenOS
Juniper SRX	Proprietary	Included on SRX security gateways	Proprietary operating system Junos
Sonicwall	Proprietary	Included on Dell appliance	Proprietary operating system SonicOS Based on the Linux kernel
Barracuda Firewall	Proprietary	Included Firewall Next Generation appliance	Windows-based appliance embedded firewall distribution
Cyberoam	Proprietary	Included Firewall Sophos appliance	Windows-based appliance embedded firewall distribution
D-Link	Proprietary	Included Firewall DFL	Windows-based appliance embedded firewall distribution
Endian Firewall	Proprietary	Free / Paid	Linux-based appliance
Forcepoint NGFW	Proprietary	Included on all Forcepoint NGFW devices	Proprietary operating system
OPNsense	Simplified BSD / FreeBSD License	Free / Paid	FreeBSD-based appliance firewall distribution
pfSense	Apache 2.0 / Proprietary (Plus)	Free / Paid	FreeBSD-based appliance firewall distribution
Zeroshell	GPL	Free / Paid	Linux/NanoBSD-based appliance firewall distribution
SmoothWall	GPL	Free / Paid	Linux-based appliance embedded firewall distribution
IPFire	GPL	Free (Donations welcomed)	Linux-based appliance embedded firewall distribution
WatchGuard	Proprietary	Included on all Firebox devices	Proprietary, Fireware OS, Based on the Linux kernel
WinGate	Proprietary	Free / Paid	Windows-based appliance embedded firewall distribution

pfSense is a firewall/router software distribution based on FreeBSD. The open source pfSense Community Edition (CE) and pfSense Plus software is installed on a physical computer or virtual machine to create a dedicated firewall/router for a network. pfSense can be configured and updated through a web-based interface and requires no knowledge of the underlying FreeBSD system to manage.

https://en.wikipedia.org/wiki/PfSense



Netgate 1100	Small Office Branch Office	ARM Cortex A53 1.2 GHz 2-Core	1GB DDR4	8GB eMMC Flash	3x 1GbE	3.48W (idle)	MORE DETAILS
Netgate 2100	Small Office Branch Office Remote Worker	ARM Cortex A53 1.2 GHz 2-Core	4GB DDR4	8GB eMMC Flash	4x 1 GbE	4W (idle)	MORE DETAILS
Netgate 3100	SOHO Network Remote Worker	ARMv7 Cortex-A9 1.6 GHz 2-Core	2GB DDR4	8GB eMMC Flash	6x 1GbE	6W (idle)	MORE DETAILS

Browser-Extensions

Individual Protection

Smartphone / Desktop

Best practice advice on keeping software up to date on smartphones, tablets, laptops and desktop PCs.

There's a huge amount of software running on modern mobile devices. This includes operating systems like Android and iOS, and the apps we install to do just about everything from word processing to photo retouching to sound recording. To prevent known vulnerabilities from being exploited, all software must be kept up to date. This means installing patches issued by software developers to close security holes found in their products. Hence the name "patching." This guide is designed to help you understand the security risks posed by outdated devices and advise you on how best to protect your devices against the latest cybersecurity threats.

You should make sure you have ways to keep each of the following major types of software up to date:

- **Operating System (OS):** Most operating systems support automatic updates, but the feature must be enabled. It is usually enabled by default, but could have been turned off.
- **Web browsers and extensions:** Web browsers are particularly vulnerable because they are very complex software and the websites you visit may exploit vulnerabilities in them.
- **Third-party apps - especially Office apps:** Apps that you install yourself need to be kept up to date. Some apps update themselves, others are updated through your device's app store, but some require you to install the updates yourself.
- **Antivirus:** If you use antivirus or endpoint security apps, make sure they are updated regularly. Like other software, antivirus updates include bug fixes and new features, but also new signatures that can detect new malware recently discovered by AV companies.

https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date

Browser-Extensions

Individual Protection

Smartphone / Desktop

Use strong passwords

Do you use any of these words as a password or in combination with a single dictionary word? If so, you need to change your password to something stronger:

Four-digit year numbers
Examples: 19XX, 20XX, other anniversaries or famous year numbers like 1776 or 1066

"password"
Examples: pass, password, p@$$word or any variant

Sports References
Examples: footballfan, field hockey, hoppfcb

Personal information
Examples: Your name, email address, phone number, or social security number.

Keyboard patterns or sequences
Examples: qwerty, asdf, 123456,abc123

Names
Examples: Pets, spouses, children, grandchildren, celebrities.

Browser-Extensions

Individual Protection

Smartphone / Desktop

Strong passwords

Do you use any of these words as a password or in combination with a single dictionary word? If so, you need to change your password to something stronger:

A good password must meet the following requirements

- One upper case English letter (A-Z)
- An English lowercase letter (a-z)
- A number (0-9) and/or a symbol (e.g. !, #, or %)
- A total of ten or more characters.

One way to do this is to start with a word you can remember:

pamphlet

Then add elements from the criteria above.

pAMPh$3let

Individual Protection

Smartphone / Desktop

Better yet: Strong passphrases

Passphrases are longer and more complex than passwords. They are easier to remember, but harder to guess.

Method A: Convert a phrase into an acronym.

Choose a phrase you can remember and reduce it to the first letters of each word, incorporating some numbers, capitalization, and punctuation.

Mccic:Iiig,web? -> Mint chocolate chip ice cream: If it isn't green, why even bother?

Method B: Unique phrase

Choose 4-5 letters (MEKL) and then make a phrase of words starting with each of those letters. Add a number or punctuation if it makes sense.

Miami!!!ItSoundsLovely

MyParentsCanLaugh?

Individual Protection

Smartphone / Desktop

Time: 1'
Task: Create a passphrase

1. Select 4 random letters
2. Create a sentence with 4 words starting with these letters
3. Make sure it contains at least 20 characters

CupcakesPlottingAgainstUs

Password Manager

Individual Protection

Smartphone / Desktop

Best: Password Manager

The clear recommendation is to use a password manager for all your online accounts. It provides additional security because it stores passwords in an encrypted and password-protected way. This password is the only one you need to remember. For the access data to each account, you can use the built-in generator to create secure, hard-to-guess character combinations. And set a separate password for each account. Optionally, many password managers allow two-factor authentication, which provides additional protection.

The commercial password managers also take care of storing and synchronizing passwords between computer and smartphone. Extensions for popular browsers such as Chrome, Safari, Firefox, Opera and Microsoft Edge allow convenient filling in of forms and credentials.

However, in password managers you can store not only access data to online services, but also other confidential information. PIN codes, credit card information or the numerical code of the bike lock can be stored securely as a note in the password manager.

https://www.swisscom.ch/de/magazin/datensicherheit-infrastruktur/passwort-manager-tipps-sicherheit/

Individual Protection

Smartphone / Desktop

KeePass
Password Safe

KeePass follows a completely different direction. The open-source password manager from German developer Dominik Reichl has numerous functions, can be extended with plug-ins, and stores passwords in encrypted files. KeePass and compatible apps are available for every conceivable operating system, including Windows, macOS, iOS, Android and Blackberry. There are also plug-ins for the most popular browsers.

However, the user has to take care of the synchronization of the password files between the devices, and the handling and browser integration are not quite as elegantly solved as in the commercial offers. Thus, KeePass is suitable for advanced users and those who distrust the password storage of the commercial providers.

bitwarden

Bitwarden is a free open-source password manager that stores confidential information such as website credentials in an encrypted vault. The Bitwarden platform offers a variety of client applications including a web interface, desktop applications, browser extensions, mobile apps and also runs in command line interpreter. Bitwarden offers a cloud-hosted service as well as the ability to self-host the service.

https://protonmail.com/blog/open-source-password-managers/

Individual Protection

Smartphone / Desktop

https://www.kaspersky.de/resource-center/definitions/what-is-a-vpn

Virtual Private Network - VPN

VPN stands for "Virtual Private Network" and describes the possibility to establish a protected network connection using public networks. VPNs encrypt your Internet traffic and disguise your online identity. This makes it difficult for third parties to follow your tracks on the Internet and steal data. The encryption process takes place in real time.

Advantages:

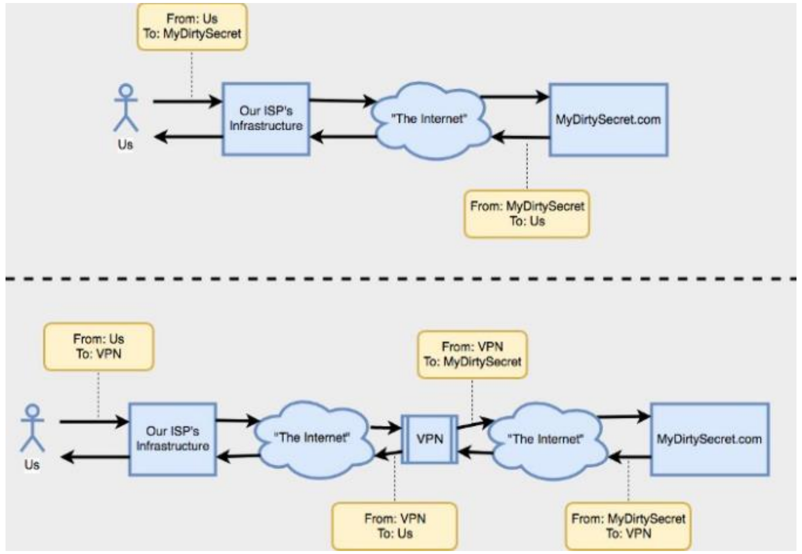
❑ Data traffic on the Internet disguised, and protected from outside access.

❑ Secure encryption: To be able to read the data, you need an encryption key (literally translated: "encryption key"). With the help of a VPN, your activities on the Internet are reliably hidden even in public networks.

❑ Concealing your location: VPN servers basically act as your representatives on the Internet. Since the demographic location data comes from the server in another country, your actual location cannot be determined. Possibly none/limited **logging**.

❑ Access to regional content, and even your own on the local network.

❑ Secure data transfer: VPN services connect to private servers and use encryption methods to reduce the risk of data leaks.



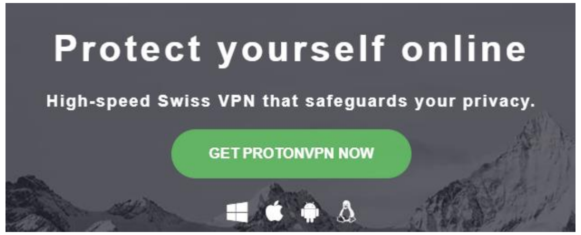
https://medium.com/tebs-lab/do-vpns-actually-protect-your-privacy-5f98a9cec90a

Individual Protection

Smartphone / Desktop

Two good options for private individuals* ☺

Cisco AnyConnect Secure Mobility Client: You need our VPN client to access all IT resources of the FHNW from abroad. You can also start the client at other universities or after connecting to SwissCom hot-spots in trains, at train stations and airports to use the internet connection for free. Paid library searches can also be carried out conveniently outside the school buildings with this connection.



Our story began at CERN, the place where the Internet was born and our founding team met. On the 25th anniversary of the Internet in 2014, we developed ProtonMail to make Internet privacy a reality again for millions of people around the world. The ProtonVPN project was created out of necessity to better protect activists and journalists who use ProtonMail.

https://protonvpn.com/

https://fhnw.ch/plattformen/it-campus-olten/anleitungen/vpn-client.html

Individual Protection

Digital Signatures

A **digital signature** - a type of electronic signature - is a mathematical algorithm routinely used to confirm the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that can be uniquely assigned to a person or company and are used to identify users and protect information in digital messages or documents. For e-mails, the e-mail content itself becomes part of the digital signature. Digital signatures are much more secure than other forms of electronic signatures.

"Occasionally when I send someone an email, they write me back that my message contains a mysterious attachment called **"signature.asc"** that they can't open. I refer such people to this page for an explanation. The "attachment" you see is actually a digital signature. Just like a physical signature on a paper document, this digital signature confirms that I am the author of the message. Unlike signed paper documents, which are relatively easy to forge or otherwise manipulate, with digital signatures you can be very sure that the message is genuine and unaltered. Digital signatures have been a standard part of email since 1996, and most email clients handle them correctly. However, there are two notable exceptions: Microsoft Outlook and Microsoft Outlook Express. These two email clients do not interpret the signature correctly and display it as an attachment that cannot be opened."

Tristan Miller, AUSTRIAN RESEARCH INSTITUTE FOR ARTIFICIAL INTELLIGENCE

https://us-cert.cisa.gov/ncas/tips/ST04-018

Individual Protection

Digital Signatures

OpenPGP is a non-proprietary format for authenticating or encrypting data using public-key cryptography. It is based on the original PGP (Pretty Good Privacy) software. In early 1997, the OpenPGP Working Group was formed in the Internet Engineering Task Force (IETF) to define this standard, which had previously been a proprietary product since 1991. Over the last decade, PGP, and later OpenPGP, has become the standard for almost all signed or encrypted email worldwide. OpenPGP also defines a standard format for certificates that, unlike most other certificate formats, enables a network of trust.

https://us-cert.cisa.gov/ncas/tips/ST04-018

PGP / GPG
Excercise

Individual Protection

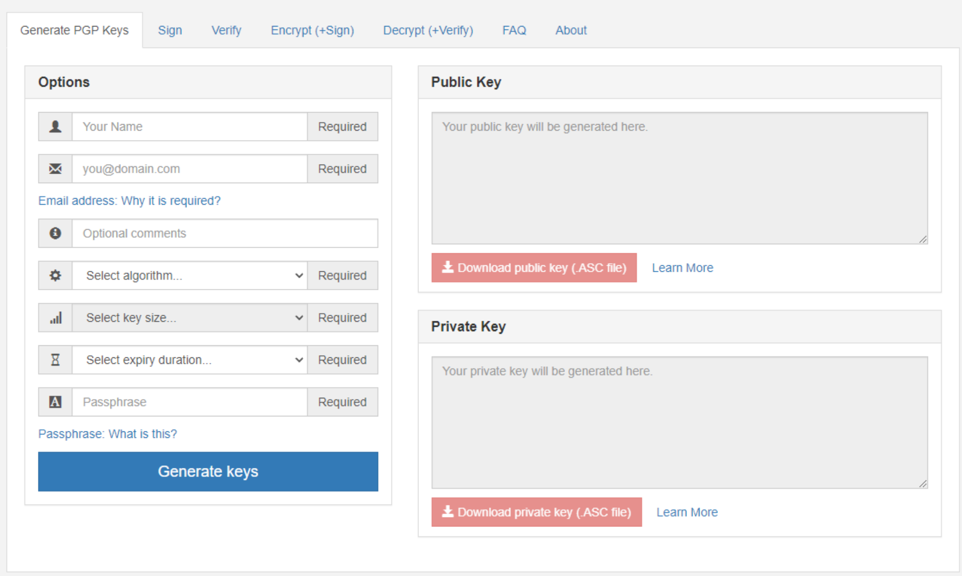
Digital Signatures

GnuGPG

Gpg4win is a Windows version of GnuPG with a context menu tool, a crypto manager and an Outlook plugin for sending and receiving standard PGP/MIME mails. The current version of Gpg4win is 3.1.16.

https://gnupg.org/

We test GPG / PGP



https://pgptool.org/

Individual Protection

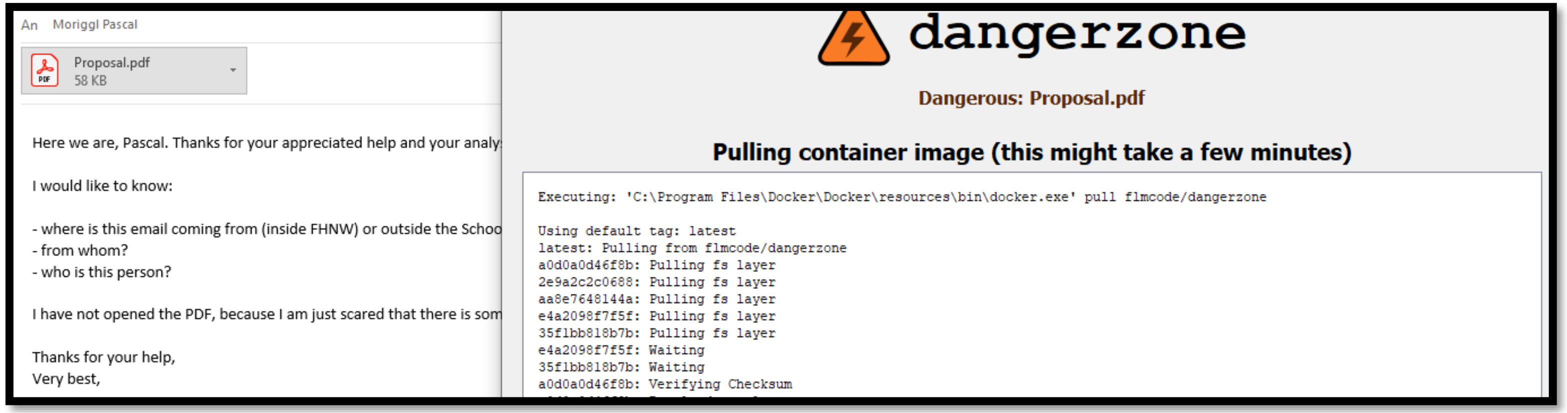
Open Attachments

Fishy Mail Received?

Virtual sandboxes (also on Windows) can be used to check PDFs. These do not show the behavior of the document, but make the content readable*.

*Rest risk present.

For example, using Dangerzone and Docker.
https://github.com/firstlookmedia/dangerzone



An Moriggl Pascal

Proposal.pdf
58 KB

Here we are, Pascal. Thanks for your appreciated help and your analy

I would like to know:

- where is this email coming from (inside FHNW) or outside the Schoo
- from whom?
- who is this person?

I have not opened the PDF, because I am just scared that there is som

Thanks for your help,
Very best,

Dangerous: Proposal.pdf

Pulling container image (this might take a few minutes)

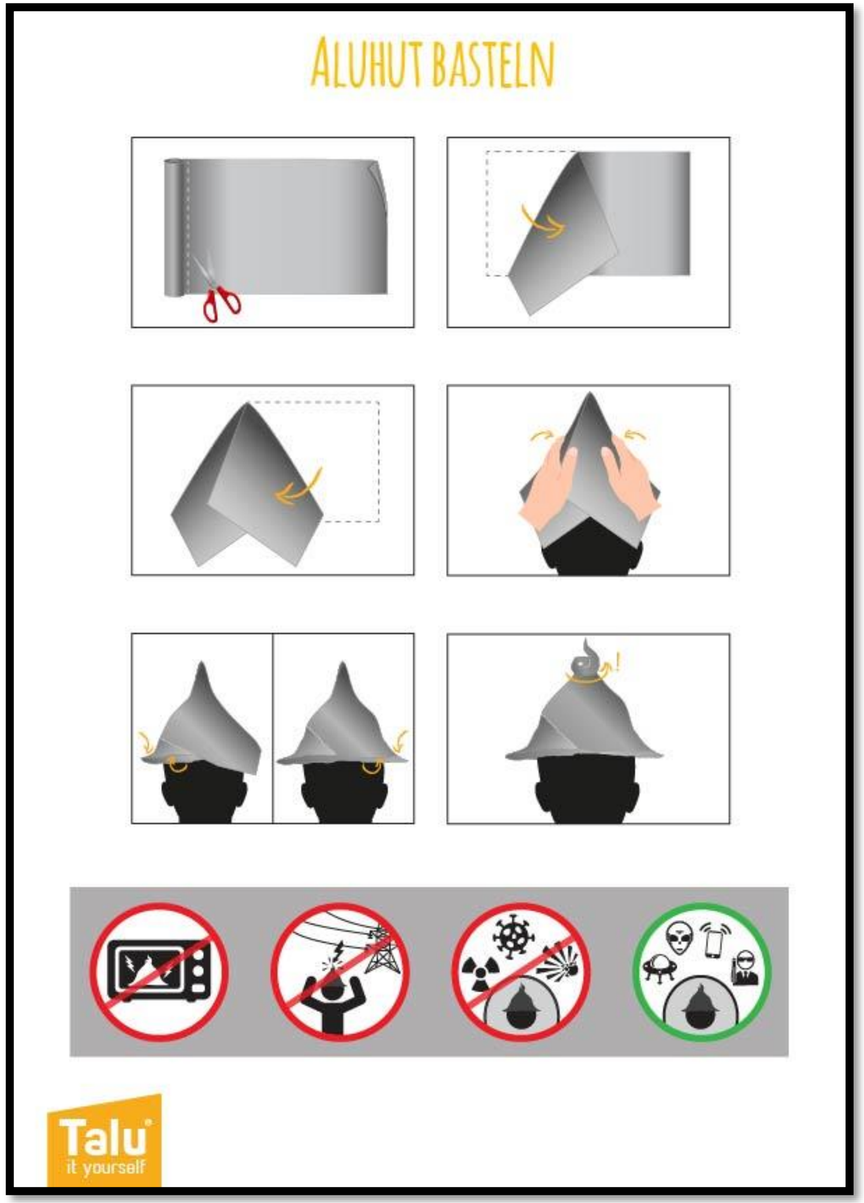
```
Executing: 'C:\Program Files\Docker\Docker\resources\bin\docker.exe' pull flmcode/dangerzone

Using default tag: latest
latest: Pulling from flmcode/dangerzone
a0d0a0d46f8b: Pulling fs layer
2e9a2c2c0688: Pulling fs layer
aa8e7648144a: Pulling fs layer
e4a2098f7f5f: Pulling fs layer
35f1bb818b7b: Pulling fs layer
e4a2098f7f5f: Waiting
35f1bb818b7b: Waiting
a0d0a0d46f8b: Verifying Checksum
```

Scalar Waves**

Individual Protection

Dont become a target

**Before the last story, please
Protect yourself wearing a
Tinfoil hut!****



Individual Protection

Dont become a target

After that: The router is a potential weak point

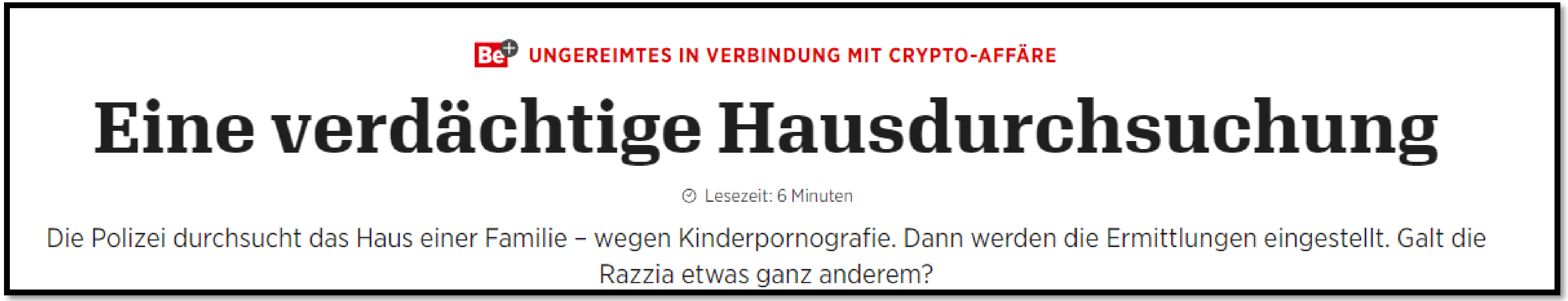
Your IP is directly associated with you, and is effectively your online identifier. Thus, your router is actually the first point worth protecting, in order to protect you with your unique IP from false, legal persecution via false flag.

Aluhut? Read the article from 10.11.2021 here:
https://www.beobachter.ch/gesellschaft/ungereimtes-in-verbindung-mit-crypto-affare-eine-verdachtige-hausdurchsuchung

Which hardware (e.g. RT-AX88U)?
https://www.amazon.com/RT-AX88U-Dual-Band-Aiprotection-Lifetime-Compatible/dp/B07HM6KJN8

Which software to put on the router:
https://www.freshtomato.org/

Which settings to make (no matter which software and hardware)
https://heimdalsecurity.com/blog/home-wireless-network-security/



Be+ UNGEREIMTES IN VERBINDUNG MIT CRYPTO-AFFÄRE

Eine verdächtige Hausdurchsuchung

Lesezeit: 6 Minuten

Die Polizei durchsucht das Haus einer Familie – wegen Kinderpornografie. Dann werden die Ermittlungen eingestellt. Galt die Razzia etwas ganz anderem?