

Sicherheit

Bei Sicherheit geht es nicht nur um technische Lösungen, sondern auch um Cyber Awareness Schulungen und Wissensvertiefung.

- [DNS-Schutz](#)
 - [PC-SPEZIALIST DNS-Schutz](#)
 - [Einstellungen des DNS-Filters](#)
 - [DNS-Schutz auf einem Apple-Gerät aktivieren](#)
 - [DNS-Schutz auf einem Android-Gerät aktivieren](#)
- [VPN](#)
 - [VPN für Privatkunden](#)
- [Sicherheitsvorfall](#)
 - [Sicherheitsvorfall melden](#)
 - [Sicherheitsvorfall aufarbeiten](#)
- [Mobile Security](#)
 - [Mobile Security FAQ](#)
- [Phishing](#)
 - [Phishing-E-Mails erkennen](#)
- [E-Mail-Sicherheit](#)
 - [Informationen über NoSpamProxy Cloud](#)

DNS-Schutz

PC-SPEZIALIST DNS-Schutz

Mobilgeräte wie Notebooks, Smartphones oder Tablets werden für den Alltag im Geschäfts- und Privatleben immer wichtiger.

Auf den Geräten sind viele sensible Daten gespeichert. Deshalb ist ein Schutz davon essenziell.

Unternehmen brauchen eine sichere, private, verwaltbare und sichtbare Kontrolle über ihren Internetverkehr.

Das derzeitige Domain Name System (DNS) löst Internetanfragen über ein globales System von Servern auf und übersetzt diese Anfragen dann in eindeutige IP-Adressen (Internet Protocol). So wird aus www.google.de (können Menschen sich merken) eine IP-Adresse (mit dieser funktioniert das Internet).

Dieser lebenswichtige Dienst wurde jedoch nicht mit Blick auf die Sicherheit entwickelt.

Daher gibt es hier inzwischen viele Angriffsmethoden und Schwachstellen.

Durch den Einsatz einer DNS-Sicherheitslösung wie PC-SPEZIALIST DNS-Schutz haben Unternehmen die Kontrolle über ihre Netzwerke und erhalten die Sicherheit, den Datenschutz und die Transparenz, die sie zum Schutz ihrer IT-Infrastruktur und ihrer Benutzer benötigen, selbst wenn diese aus dem Home Office arbeiten.

Eine Absicherung über Verbindung in das Firmennetz über VPN ist nicht immer möglich und klassische Virenschutzlösungen sind auf Smartphones wenig sinnvoll.

Deshalb haben wir mit PC-SPEZIALIST DNS-Schutz eine Lösung erschaffen, die Bedrohungen bereits auf DNS-Ebene erkennt und blockiert. Wenn Sie z.B. `schadhafte.website.de*` aufrufen, wird schon die Auflösung zu dem dahinterliegenden Server fehlschlagen und Sie bleiben so geschützt. Die Website kann dann nicht geöffnet werden.

Obwohl sich das Produkt eher an Geschäftskunden orientiert, richten wir es sehr gerne auch für Privatkunden ein.

Unsere Lösung unterstützt die Plattformen Windows, macOS, Linux, ChromeOS, Android, iOS sowie einige Router und Browser.

Monitoring und Wartung sind nur in Kombination mit unserem Eins-für-alles-Paket für Windows enthalten.

Damit der Einsatz reibungslos abläuft und der Aufwand in der Konfiguration und Wartung der Produkte minimal ist, stellt die Systempartner Computervertriebs GmbH&Co.KG ihren Kunden das

Produkt zur Verfügung und verwaltet dieses.

*Beispiel - keine echte Website

DNS-Schutz

Einstellungen des DNS-Filters

Über diesen [Link](#) können Geschäftsführende Einstellungen des DNS-Filters vorschlagen.

DNS-Schutz auf einem Apple-Gerät aktivieren

- Navigieren Sie zu apple.nextdns.io
- Füllen Sie die Felder **Profile**, **Device Name** und **Device Model** aus und haken Sie unten **Sign Configuration Profile** an
- Die ID des Profils erhalten Sie von uns



Set up NextDNS natively on Apple devices

Generate a configuration profile (.mobileconfig) and install on any Apple device to set up NextDNS on all networks.

Profile

abc123

Device Name

Identify your device in Analytics and Logs.

Test's iPhone

Device Model

iPhone

iPad

Macbook

Mac

Apple TV

iPhone 15 Pro Max

Excluded Wi-Fi Networks

Wi-Fi networks (SSID) on which NextDNS is disabled.

My Home Network, My Work Network, ...

Excluded Domains

Domains that will bypass NextDNS and use the network-provided DNS.

intranet.company.com, myprinter.lan, ...

☐ Trust NextDNS Root CA

Remove the HTTPS warning when loading the block page. Make sure you are aware of the implications of trusting a third-party root CA.

☐ Bootstrap IPs

Enable this if your network is blocking NextDNS. This may result in higher latency.

☒ Prohibit Disabling

Prohibit users from disabling NextDNS.

☒ Sign Configuration Profile

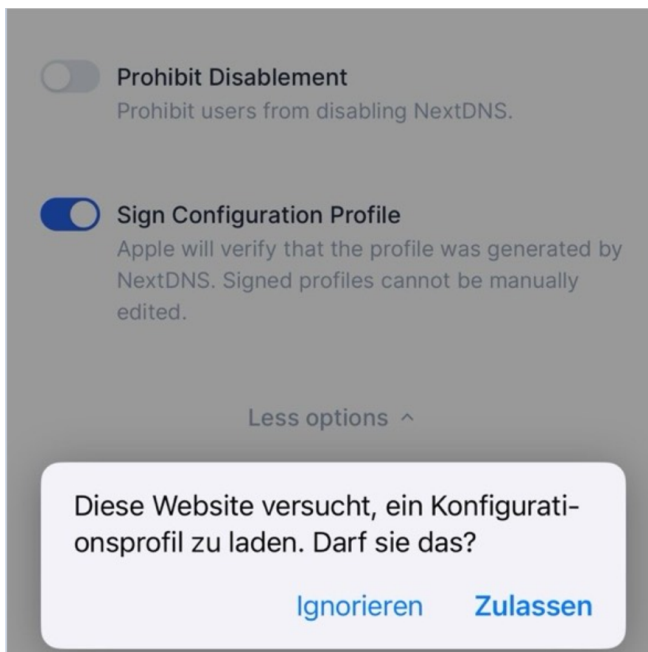
Apple will verify that the profile was generated by NextDNS. Signed profiles cannot be manually edited.

Less options

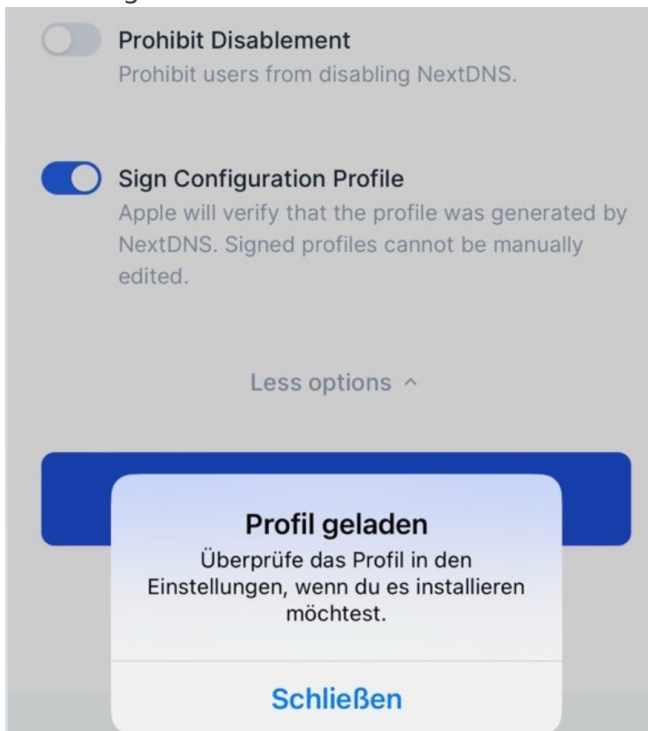
Download

or generate a [short link](#) or [QR code](#)

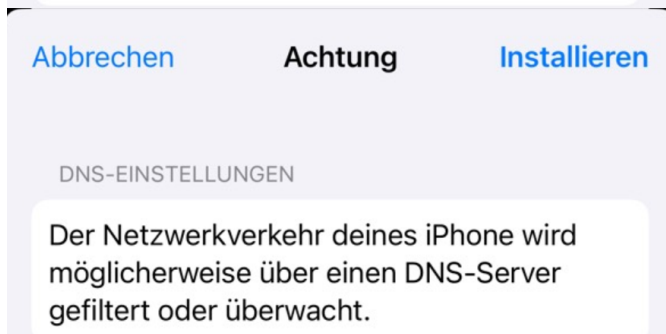
- Klicken Sie auf **Download**
- Erlauben Sie den Download mit Klick auf **Zulassen**



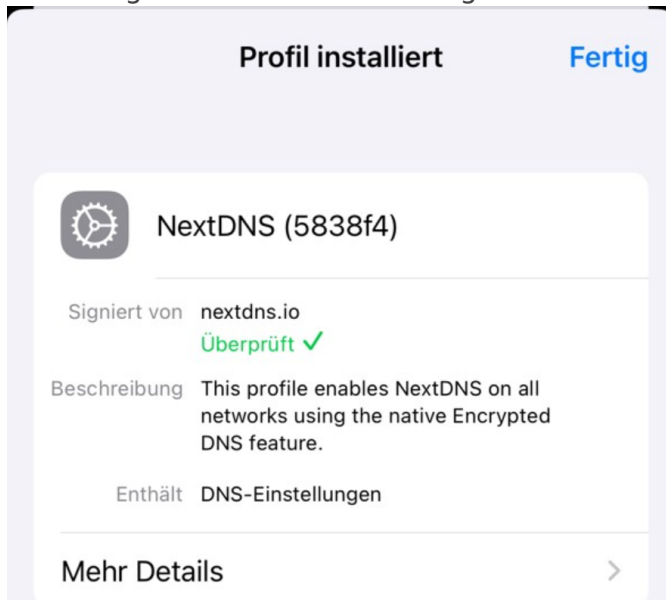
- Bei erfolgreichem Download sehen Sie die Meldung **Profil geladen**



- Öffnen Sie nun die App **Einstellungen** und installieren Sie dort das heruntergeladene Profil mit Klick auf **Installieren**



- Bei Erfolg sollten Sie die Meldung **Profil installiert** sehen



- Sie sind nun geschützt 

DNS-Schutz auf einem Android-Gerät aktivieren

- Gehen Sie zu **Einstellungen** → **Netzwerk & Internet** → **Erweitert** → **Privates DNS**
- Wählen Sie die Option **Hostname** des Anbieters für privates DNS
- Geben Sie die von uns mitgeteilte Adresse ein (z.B. Smartphone-abc123.dns.nextdns.io) und klicken Sie auf Speichern

17:20



Privaten DNS-Modus auswählen

- ☐ Aus
- ☐ Automatisch
- ☒ Hostname des privaten DNS-Anbieters

Smartphone-abc123.dns.nextdns.io

ABBRECHEN SPEICHERN

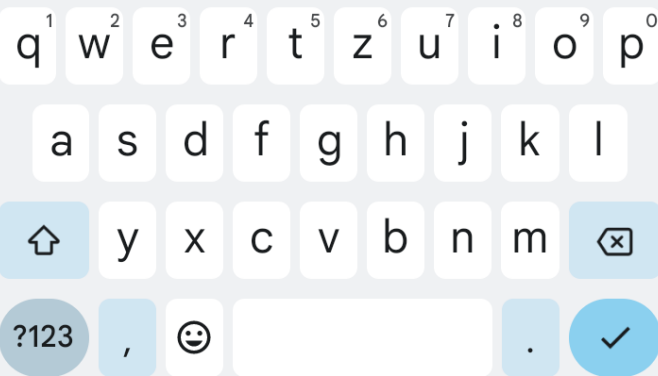


Hotspot und Tethering

Aus



GIF



VPN

VPN für Privatkunden

Klassischerweise denken wir bei einem VPN an die Verbindung in das eigene Netz. Insbesondere bei Firmen ist das ein gängiger Standard, um einen sicheren Zugriff außerhalb des Firmenstandort zu gewährleisten.

Es gibt aber auch die Möglichkeit, ein VPN zu nutzen, um sich angeblich anonym im Internet zu bewegen oder Sperren zu umgehen. Meistens raten wir von solch einem Anwendungsfall ab, da eine anonyme Nutzung nur mit einer Anpassung der Nutzungsgewohnheiten möglich ist und die reine Nutzung von einem VPN nichts bringt. Außerdem gibt es in den meisten Ländern keine Sperren zu seriösen Inhalten. **In den meisten Fällen sollte also auf ein VPN verzichtet werden.**

Falls aber doch ein VPN von einem externen Anbieter gewünscht ist, empfehlen wir den Anbieter



[Mullvad VPN](#). Folgende Eigen

schaften finden wir dort super:

- Kein Marketing / keine Werbung
- Keine Protokollierung und anonyme Konten
- Unabhängige Audits und offener Quelltext
- Keine unrealistischen Versprechen
- Ausschließlicher Fokus auf VPN (bei vielen anderen Anbietern ist VPN nur ein *Zusatz* zu Virenschutz, Cybervesicherung, Dark Web Monitor, Passwortmanager und anderen Services, die eigentlich nichts mit VPN zu tun haben)

Bei näherem Interesse gibt es in dem [Artikel bei heise](#) oder dem [Video](#) weitere Details.

Die Installation ist über unser **Eins-für-alles-Paket automatisiert** (Windows und macOS). Wie beim Eins-für-alles-Paket beträgt die Laufzeit bei uns 1 Jahr. Kürzere oder längere Laufzeiten können Sie gerne selbst erwerben. Eine Bestellung der Lizenz über uns erfolgt per **Vorkasse** und dauert ungefähr eine Woche nach Zahlungseingang.

Für Linux, [iOS](#) und [Android](#) gibt es die Anwendungen im [Downloadbereich](#).

Unterstützung bieten wir zu unserem normalen Stundensatz an. Da die Anwendung nur in Ausnahmefällen im Einsatz ist, kann unter Umständen nur mit einer zeitlichen Verzögerung geholfen werden. Melden Sie sich gerne bei Fragen per E-Mail oder telefonisch.

Sicherheitsvorfall

Sicherheitsvorfall

Sicherheitsvorfall melden

Melden Sie uns einen Sicherheitsvorfall über das [Sicherheitsvorfall-Formular](#).

Sicherheitsvorfall

Sicherheitsvorfall aufarbeiten

Mobile Security

Mobile Security FAQ

- Können die Daten aus dem privaten Container auf ein neues Smartphone übertragen werden?
 - Nein, die Daten dort lassen sich nicht übertragen. Achten Sie also darauf, dass wichtige Daten über die Cloud synchronisiert werden.
- Können Daten mit Samsung Smart Switch von einem privaten Smartphone in das private Profil eines Firmensmartphones (COPE) übertragen werden?
- Können die Dienstmartphones aus der Ferne gelöscht werden?
- Können die Dienstmartphones geortet werden?
- Wird der Datenverkehr überwacht?

Phishing

Phishing-E-Mails erkennen

Es gibt mehrere Anzeichen für Phishing-E-Mails, die wir hier regelmäßig aktuell aufführen.

- **Gefälschter Absender**

- -----Ursprünglicher Termin-----
Von: Microsoft Rechnungswesen <subscription.320836655211@email22HU.ssl.acehsport.wiki> **Im Auftrag von** Microsoft Rechnung
Gesendet: Donnerstag, 15. Mai 2025 10:35
An: Microsoft Rechnungswesen; Info; Lizenzmanager
Betreff: Thank You for Renewing Your Microsoft Office365 Subscription
Zeit: Freitag, 16. Mai 2025 12:00-13:00 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien.
Ort: Microsoft Verwaltungsportal für Abrechnung

- **Ungewöhnliches Format**

- -----Ursprünglicher Termin-----
Von: Microsoft Rechnungswesen <subscription.320836655211@email22HU.ssl.acehsport.wiki> **Im Auftrag von** Microsoft Rechnung
Gesendet: Donnerstag, 15. Mai 2025 10:35
An: Microsoft Rechnungswesen; Info; Lizenzmanager
Betreff: Thank You for Renewing Your Microsoft Office365 Subscription
Zeit: Freitag, 16. Mai 2025 12:00-13:00 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien.
Ort: Microsoft Verwaltungsportal für Abrechnung

- Rechnung kommt als Kalendereintrag und/oder mit HTML-Dokument anstatt PDF

- **Unerwartete E-Mail**

- -----Ursprünglicher Termin-----
Von: Microsoft Rechnungswesen <subscription.320836655211@email22HU.ssl.acehsport.wiki> **Im Auftrag von** Microsoft Rechnung
Gesendet: Donnerstag, 15. Mai 2025 10:35
An: Microsoft Rechnungswesen; Info; Lizenzmanager
Betreff: Thank You for Renewing Your Microsoft Office365 Subscription
Zeit: Freitag, 16. Mai 2025 12:00-13:00 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien.
Ort: Microsoft Verwaltungsportal für Abrechnung

- Die Abrechnung des Dienstes erfolgt über einen Partner wie uns (z.B. Microsoft 365) oder es ist aktuell keine Lieferung bestellt (z.B. Lieferinformation von DHL)

- **Bedrohlicher Text mit Drohung/Warnung**

- Phishing-E-Mails sind meistens angeblich kritisch und vermitteln Druck

P.S. Wir bieten eine leistungsstarke E-Mail-Schutzlösung, die wir als Ergänzung zu Microsoft 365 anbieten. Sprechen Sie uns gerne darauf an.

E-Mail-Sicherheit

E-Mail-Sicherheit

Informationen über NoSpamProxy Cloud

Digitale Souveränität

<https://www.youtube-nocookie.com/embed/cT1zdx5V98E?si=fuWorcvaWygYf4XO>