

# Zur Abwechslung mal eine „Virenwarnung“



Anzeige ist auf „Schreck“  
gebürstet

Don't worry, dies ist nur ein mieser  
Fake, aber kein Virus

Nicht anrufen, sonst haben Sie  
echt Trouble

[Wie Sie diese Anzeige entfernen,  
siehe weiter unten...](#)

# Nur noch lästig, sofort löschen



**McAfee™**  
Together is power.

**Prioritäre E-Mail:** \*\*\*\*\*@t-online.de

**Ihr Abonnement ist abgelaufen !!**

Wir haben mehrmals versucht, mit Benachrichtigungen und Warnungen auf Ihr Konto zuzugreifen, haben jedoch keine Antwort von Ihnen erhalten. Erneuern Sie Ihr Abonnement, da Sie nicht mehr vor Cyberangriffen und Hackern geschützt sind. Zu Ihrer eigenen Sicherheit empfehlen wir Ihnen dringend, Ihr Abonnement zu erneuern. Wenn Sie Ihre Mitgliedschaft nicht verlängern, wird Ihr Konto innerhalb von 48 Stunden geschlossen.

**AUSWEIS:** \*\*\*\*\*  
**E-mail:** \*\*\*\*\*@t-online.de

[Hier Weitermachen](#)

**Wenn keine Maßnahmen ergriffen werden, wird Ihr Konto innerhalb von 48 Stunden geschlossen.**

---

Im Rahmen unseres Treueprogramms erhalten Sie einen **RABATT:**  
**Bis zu 80 % Rabatt**



**McAfee™**  
Gemeinsam ist Macht.

**LETZTE MAHNUNG:**

**BESTÄTIGUNG ERFORDERLICH**

Ihr Subscription von McAfee Total Protection endet möglicherweise bald

Nach Ablauf des Enddatums werden unsere Geräte für Hacker angreifbar ...

---

**Datum endet: Bald**

---

**Schützen Sie Ihre Geräte JETZT >>>**

✓ **Verfügbar** : (-95%) Noch heute Verlängerungsrabatt

Erneuern Sie Ihr Subscription, indem Sie auf die Schaltfläche unten klicken:

[Jetzt aktivieren](#)

**Notiz:** Wenn kein Subscription registriert ist, wird Ihr Konto möglicherweise innerhalb von 48 Stunden als inaktiv markiert.

Betrug: Anzeige soll nur kostenpflichtiges Abo auslösen. Wie Sie diese entfernen, siehe weiter unten...

## Kritische Sicherheitswarnung

QrRvJPP6xSP1uBFkXOM4MSHOFd7SGW@seoul-rp.net 3 Stunden geschlossen. ! [ID-N.317177136]\*312984  
| T-ONLINE | PRIORITÄTSMAIL: =>waeggfsh |  
An: waeggfsh@t-online.de

 telekom.de

KRITISCHE SICHERHEITSWARNUNG:  
**Ihr Schutz ist abgelaufen!**

Hallo,

Deutsche Telekom hat **aktive Schadsoftware-Infektionen** auf Ihrem Gerät **JETZT** erkannt.

Ihr System ist kompromittiert und befindet sich in einem **hohen Risiko** für Datendiebstahl, Identitätsdiebstahl und weitere Angriffe. **Eine sofortige Entfernung ist erforderlich.**

### Gefundene Bedrohungen:

- Trojan.Stealer
- Spyware.Keylog
- Adware.Injector
- Weitere Hochrisiko-Schadsoftware

QrRvJPP6xSP1uBFkXOM4MSHOFd7SGW@seoul-rp.net

Sie haben diese dubiose Meldung von T-Online erhalten. Logischerweise müsste die Adresse von T-Online in der Absenderzeile erscheinen. Dem ist nicht so (s.o.). Länderkennung **RP** stammt von **Republik Polen**. **Also Nonsense**

**Nur löschen!**

[Anzeige ist nonsense. Wie Sie diese entfernen, siehe weiter unten...](#)

Bei diesen Anzeigen handelt es sich wahrscheinlich nicht um eine echte Infektion Ihres PCs, sondern um eine falsche Browser-Benachrichtigung (Spam/Scam).

Schädliche Websites bringen Nutzer oft dazu, auf "**Zulassen**" bei Benachrichtigungs-Anfragen zu klicken. Danach sendet die Website über die Windows-Benachrichtigungs-zentrale **Pop-ups, die wie echte McAfee-Virenwarnungen aussehen**, um Sie zum Kauf von Abos oder zum Herunterladen echter Schadsoftware zu verleiten. Dass das Phänomen nur im Microsoft Edge auftritt, bestätigt diesen Verdacht.

So entfernen Sie diese störenden Benachrichtigungen in Microsoft Edge:

1. Öffnen Sie Microsoft Edge.
2. Klicken Sie oben rechts auf die drei Punkte (...) und wählen Sie Einstellungen.
3. Wählen Sie in der linken Menüleiste Cookies und Websiteberechtigungen.
4. Scrollen Sie zum Bereich Berechtigungen und klicken Sie auf Benachrichtigungen.
5. Unter dem Punkt Zulassen sehen Sie eine Liste von Websites.
6. Suchen Sie nach verdächtigen Adressen (oft unbekannte Domains wie z. B. notification-system.com, check-cleaner.net oder unseriöse Namenskombinationen).
7. Klicken Sie rechts neben der jeweiligen Adresse auf die drei Punkte (...) und wählen Sie Entfernen oder Blockieren.

### **Zusätzlicher Schutz: Browser-Daten bereinigen**

Um sicherzugehen, dass keine verbliebenen Website-Reste die Meldungen erneut auslösen:

1. Gehen Sie in den Edge-Einstellungen links auf Datenschutz, Suche und Dienste.
2. Scrollen Sie zu Browserdaten löschen und klicken Sie auf Wählen Sie aus, was gelöscht werden soll.
3. Wählen Sie als Zeitspanne **Gesamte Zeit**.
4. Setzen Sie einen **Haken** bei Cookies und andere Websitedaten sowie Zwischengespeicherte Bilder und Dateien.
5. Klicken Sie auf Jetzt löschen.

Nach diesen Schritten sollten die **McAfee-Pop-ups beim Starten von Edge vollständig verschwunden sein**. Wenn Sie zur Sicherheit dennoch einen kostenlosen Virenskan durchföhren möchten, nutzen Sie dafür den integrierten Windows Defender (über das Startmenü nach Windows-Sicherheit suchen).