# Gibt es ein Malware Antivirus was gut ist?

### Beitrag von „stronca“ vom 22. Februar 2023, 22:50

Hinwollte mal wissen ob es ein gutes Malware-Antivirus program gibt für mein Mac?Hab seid heute immer komische Meldungen bekommen zb Ihre Daten wurden gestohlen usw.Danke

---

### Beitrag von „bluebyte“ vom 23. Februar 2023, 00:45

Das lässt sich manuell am besten überprüfen

Schau zuerst von wem diese Mails stammen (siehe Bildschirmfoto)

Fahre dazu mit dem Cursor auf den Absender. Die Farbe vom Absender ändert sich.

Jetzt machst du einen Rechtsklick und es öffnet sich ein Pulldown-Menü.

Oben wird dir die Adresse angezeigt. Da müssten schon die Alarmglocken klingeln.

Jetzt kannst du noch sämtlich Nachrichten nach dem Absender durchsuchen lassen.

Im Fenster Top-Treffer werden dir die Ergebnisse angezeigt. Alle Ergebnisse von genau demselben Absender. Also alles Spam und Phishing. Besondere Vorsicht ist im Moment bei Paketdiensten geboten.

Prüfe, ob deine Mail-Adresse beim Absender hinterlegt ist

Dafür braucht man sich nicht unnötig Ballast auf den Rechner knallen.

Das bekommt man als Benutzer besser geregelt als jedes Programm.

Trenne Wichtiges von Unwichtigem

Registriere mindestens 4 Mail-Accounts bei unterschiedlichen Anbietern

Für Anmeldungen in Sozialen Netzwerken nutze niemals Mail-Adressen, die du auch für PayPal oder für die Kommunikation mit deiner Hausbank nutzt.

Beispiel:

Erste Adresse kennt nur deine Hausbank

Zweite Adresse kennt nur Paypal

Dritte Adresse kennen nur Online-Geschäfte

Vierte Adresse nur für Soziale Netzwerke

Fünfte Adresse für "Cloud and Streaming"

Eine gute Portion gesunder Menschenverstand ist besser als jede KI.

Ich bekomme manchmal Phishing-Nachrichten angeblich von Ebay, PayPal oder Amazon

"Überprüfen sie ihren Account ..." oder auch "Ändern sie ihr Passwort" , blablabla

Das Kuriose daran ist, dass ich die Nachrichten auf Konten empfange, die dort nicht registriert sind.

Im Zweifelsfall Leak-Checker nutzen.

https://leakchecker.uni-bonn.de/

Einfach mal informieren

https://www.watchlist-internet...r-betruegerischen-e-mail/

Leute, die andauernd Langeweile oder zuviel Zeit haben, können sich mit Linux und DynDNS einen eigenen Heim-Mail-Server mit theoretisch unendlich vielen Mailadressen stricken

---

### Beitrag von „apfel-baum“ vom 23. Februar 2023, 01:10

hier kannst du auch noch gucken - https://haveibeenpwned.com/

lg

---

### Beitrag von „stronca“ vom 23. Februar 2023, 08:42

Also habe meine email getestet.Als Ergebnis habe ich bekommen

## Good news — no pwnage found!

---

### Beitrag von „Harry69“ vom 23. Februar 2023, 09:37

....

Erste Adresse kennt nur deine Hausbank

Zweite Adresse kennt nur Paypal

Dritte Adresse kennen nur Online-Geschäfte

Vierte Adresse nur für Soziale Netzwerke

Fünfte Adresse für "Cloud and Streaming"

Genau, und wenn ich dann fertig bin mit der Registrierung bei zwölfundrölfzig E-Mail Anbietern und dem Ausdenken von zwölfundrölfzig E-Mail Adressen und natürlich zwölfundröflzig Passwörtern und dann noch Zeit habe, bastel ich mir auch noch einen Alu Hut.

Mann, Mann...

Man kann es aber auch übertreiben.

Ich habe seit Anbeginn des Internetz lediglich zwei E-Mail Adressen. Eine für offizielle Kommunikation und eine für den Rest und habe dabei noch nie irgendwelche Probleme gehabt.

Und ich nutze auch alles was es im Bereich E-Commerz gibt. Von Amazon bis Kleinanzeigen und natürlich zig Foren.

Einfach Hirn einschalten und nicht auf jeden Mist draufklicken. Fertig.

---

## Beitrag von „stronca“ vom 23. Februar 2023, 10:04

Also erstmal drücke ich nichts was misst ist!!!Benuzte nur Facebook Ebay YouTube .Irgend welche Underground Seiten garnicht wegen solche Sachen .

---

## Beitrag von „Harry69“ vom 23. Februar 2023, 10:17

Du kannst mal den Bitdefender Virusscanner aus dem AppStore installieren und einen Scan deines Mac machen lassen.

Vielleicht hilft das ja schon.

---

## Beitrag von „bluebyte“ vom 23. Februar 2023, 11:39

Harry69 wenn du meinst, dass du damit zurecht kommst. Bitte!

Wenn du meinst, dass das übertrieben erscheint. Bitte!

Eigentlich nennt man das Standard in der IT.

Ich habe doch selbst geschrieben, dass eine gute Portion gesunder Menschenverstand mehr bewirkt als jede KI. Außerdem habe ich dieses noch anhand von Bildschirmfotos verdeutlicht. Ich muss dazu sagen, dass ich diese Mail-Adresse schon seit 1997 nutze.

Die Phishing-Mails sind heute so gut programmiert. Da kannst du scannen bis du schwarz wirst. Die Benutzer wiegen sich, bei Verwendung solcher Programme, in trügerischer Sicherheit.

stronca auch ich bewege mich nicht auf dubiosen Untergrund-Seiten.

Da reicht schon die Registrierung von Kundenkarten bei Payback, Saturn, Media Markt, etc.

Oder die Registrierung von Hardware oder Software. Schon ist man in einer der vielen Verteilerlisten. Mit irgendwelchen anrüchigen Seiten hat das heute nichts mehr zu tun.

Ernsthafte Probleme hatte auch ich in den vergangenen 30 Jahren noch nicht.

---

## Beitrag von „mhaeuser“ vom 23. Februar 2023, 11:46

Harry69 Mit Apple Hide My Email und iCloud Passwords geht ein Passwort und eine E-Mail-Adresse pro Dienst wahrscheinlich einfacher, als dir nur ein einzelnes, gutes Passwort auszudenken. Braucht sogar nicht mal einen Aluhut, weil meine alte Adresse 20-mal mehr Spam und Scams als wirkliche Nachrichten bekommt.

---

## Beitrag von „ozw00d“ vom 23. Februar 2023, 13:02

Ich nutze lediglich clam in demand und 2 x Woche fest.
Keine zusatztools nötig.

---

## Beitrag von „stronca“ vom 23. Februar 2023, 20:00

Was ist den clam in demand?

---

### Beitrag von „karacho“ vom 23. Februar 2023, 20:14

stronca Er meint bestimmt das hier -> https://www.clamav.net/

Und mit 'on demand' meint er sicher, das er es selber ab und zu manuell anwirft und scannt.

---

### Beitrag von „stronca“ vom 23. Februar 2023, 20:21

Aso jetzt weiss ich bescheid. Danke

---

### Beitrag von „karacho“ vom 23. Februar 2023, 20:25

Ich schrieb 'er meint bestimmt', ich schrieb nicht das es auch so ist Warte also erstmal, was er dazu sagt.

---

### Beitrag von „swissborder“ vom 23. Februar 2023, 21:42

LuLu von Objectiv-see ist ein schlakes Tool, welches erlaubt ausgehende Verbindungen von Programmen zu kontrollieren. Es ist erstaunlich wieviele Dienste „nach Hause telefonieren“ wollen. Eingefangene Malware würde da idealerweise geblockt. Das ist aber auch kein Freipass für unvorsichtiges Handeln.

---

## Beitrag von „Arkturus“ vom 23. Februar 2023, 22:00

Stiftung Warentest hat in der aktuellen Ausgabe 03/23 gute Tools auch für Mac angepriesen.

---

## Beitrag von „ozw00d“ vom 24. Februar 2023, 07:30

stronca es sollte on demand heissen. Clam ist ein Viren Scanner der sich sehr gut mit macOS verheiraten lässt.
fehler kam durch die Autokorrektur meines iPhones.

---

## Beitrag von „gllark“ vom 24. Februar 2023, 14:59

Schau dir mal KnockKnock an

https://objective-see.org/products/knockknock.html

Kommt vom gleichen Entwickler wie Lulu und ist kostenlos. Großartiges Tool.

---

## Beitrag von „G.com“ vom 25. Februar 2023, 11:16

Zunächst wäre ich bei Mac immer etwas entspannter. Sind die Meldungen Mails, handelt es sich zu 90% um Phishing. Mails genau lesen, Absendeadresse prüfen, ggf. E-Mail Header checken.

Sind es Meldungen in der Nachrichtenzentrale, hat man auf ner falschen Seite einJa geklickt oder es hat sich selber eingecheckt (eher unwahrscheinlich).

Dann würde ich mir Malwarebytes wine Suche starten.

Danach den Trendmicro Housecall nutzen.

Sollten weiterhin Bedenken bestehen, MacOS einfach neu drüberbügeln oder Fresh Install und Migration.

Es ist möglich aber eher unwahrscheinlich, dass sich bei MacOS etwas tief einnistet ohne Zutun des Users. Das ist der Vorteil eines Sandbox Systemes. Ist man mit nem Hacky unterwegs und hat alle Security abgeschaltet…tja, da kann man dann nur hoffen.

Viel Erfolg!

---

## Beitrag von „stronca“ vom 26. Februar 2023, 01:27

Bin mit ein MacBook Air unterwegs.Es kommen immer nur Meldungen.Alle meine Emails sind keine verdichte sachen drinnen .

---

## Beitrag von „ozw00d“ vom 26. Februar 2023, 08:33

Neben knock knock gibts vom selben Hersteller:
ransomwhere z.b.

Einfach mal auf der Seite schauen.

auSserdem würde ich am mac niemals als Admin arbeiten.

Für die täglichen Dinge reicht ein Standard Account.

Ansonsten einfach mal im Netz nach macOS hardening schauen.
gibt da Menge was man tun kann.

Ich hab zb. Immer einen Account im Paranoia Mode laufen.

Ansonsten gilt installiere nichts von Quellen denen man nicht traut.
traue keiner Mail deren Absender du nicht kennst.
Besuche keine Webseiten welche dir schaden könnten.

Sehr gut sind für bad things vms.
einfach eine erstellen ohne Zugriff auf das Dateisystem. Bestenfalls ein linux (arch zb. ).
damit kann man dann auch eben erwähntes Testen.

Es gibt auch jede Menge forensik Software welche frei erhältlich ist und man sein System auf Herz und Nieren testen kann.

Pentesting für sich selbst, sein Netzwerk etc.

Es gibt so viel was man im Netz dazu finden kann.

ein guter Einstieg https://github.com/drduh/macOS-Security-and-Privacy-Guide

---

## Beitrag von „user232“ vom 26. Februar 2023, 08:46

Ich nutz zum Scan nur EtreCheck

---

## Beitrag von „sunraid“ vom 26. Februar 2023, 09:37

Wie sieht es eigentlich mit der integrierten Software XProtect (Version 2166 soll ja gerade neu installiert worden sein) aus?

Kann man die Installation auch manuell anstoßen? Bei mir unter Monterey wird unter Installationen noch die 2159 angezeigt.

---

### Beitrag von „user232“ vom 26. Februar 2023, 10:02

schau dir mal XProCheck an

Edit:

Kann nur XProtect anstoßen zu scannen, schau dir vlt auch mal SilentKnight dazu an (gleiches Entwicklerteam)

---

### Beitrag von „guckux“ vom 27. Februar 2023, 14:26

Da hier über Malware und so getalkt wird - heise hat dazu auch was reported...

Will hier niemanden was unterstellen 

---

### Beitrag von „Arkturus“ vom 27. Februar 2023, 17:52

> Zitat von guckux
>
> Da hier über Malware und so getalkt wird - heise hat dazu auch was reported...
>
> Will hier niemanden was unterstellen

die bei Heise beschriebenen Scenarien setzen quasi die Beschaffung gekrackter Software aus dubiosen Quellen voraus. Sehe ich das richtig?

---

### Beitrag von „guckux“ vom 27. Februar 2023, 19:42

Correctement...

ich wollte es nur der Vollständigkeit halber angemerkt haben, ist ja im Prinzip gängige Praxis seit gut nem Vierteljahrhundert...

---

### Beitrag von „Arkturus“ vom 27. Februar 2023, 19:44

um so etwas zu vermeiden kam ich von Windows über Linux zum macOS

---

### Beitrag von „guckux“ vom 27. Februar 2023, 20:38

Ich habe es damals nicht gemacht und Resultat war über die >30 Jahre guten 5-stelligen Betrag teils noch im Regal stehen zu haben... letztlich habe ich 2mal in den 90igern nen Virenbefall gehabt - woher auch immer - und seitdem nicht mehr wieder

---

### Beitrag von „karacho“ vom 3. März 2023, 21:50

> Zitat von swissborder
>
> LuLu von Objectiv-see ist ein schlakes Tool,

...Version 2.4.2 vom 28.06.2022. Gut gemeint, aber nicht mehr auf der höhe der Zeit.

---

## Beitrag von „ozw00d“ vom 4. März 2023, 08:31

Mal im Ernst: wenn ich so auf meinen Beruf schaue bringt dir kein antimalware etc. überhaupt etwas.
in allen Fällen in den ich es mit cyberkriminalität zu tun hatte (Ransomwhere, Trojaner und Viren) brachte kein antivir/antimalware Tool irgendwas.

Egal ob sophos, defender (nicht die azure Version), Norton oder sonstwas konnte den Dingern irgendwas anhaben.

Die Aussage eines forensikers hat mich weitestgehend erleuchtet : willst du es sicher haben, muss der netzwerkverkehr mitgeschnitten, abgefangen und in Echtzeit analysiert werden.

Alles was an Aktiver antivir/antimalware kann ist die scheisse erst dann zu erkennen wenn er dir quasi auf den Schreibtisch geschissen hat.

Also keep calm hab ein achtsames Auge, vertraue keinen Fremden oder illegalen Quellen. Jede email die nicht erwartet wurde ist ein potentielles Sicherheitsrisiko.

Ich kann diese Panik als paranoider it Mensch nicht verstehen. Es gibt nicht das Tool was hilft. Dazu gehört etwas mehr hirnschmalz als nur stupide irgend ein Tool zu installieren und sich darauf zu verlassen.