

# Malwareinfektion

Ein Antivirenprogramm und ein automatisch aktualisiertes Betriebssystem sind unabdingbar, um im Internet sicher surfen zu können. Dennoch kann es vorkommen, dass sich ein Computer mit Malware infiziert. Erkennen Sie dies und reagieren Sie richtig!

## Wie erkenne ich eine Malwareinfektion?

### Mögliche Indizien:

- Infektionsmeldung des Antivirenprogramms.
- Fehlermeldungen beim Starten oder Herunterfahren des Computers.
- Der Computer läuft nicht mehr stabil – häufige Abstürze.
- Langsames System, ständige Auslastung des Arbeitsspeichers und/oder des Prozessors, ständige Festplattenaktivität.
- Das Antivirenprogramm ist deaktiviert (auch nachdem Sie es explizit aktiviert haben).
- Die Webseite eines oder mehrerer Antivirenhersteller kann nicht mehr erreicht werden.

Wie Sie sich vor einer Malwareinfektion schützen, können Sie im [«Schritt 2 – überwachen»](https://www.ebas.ch/2-ueberwachen-mit-virenschutz-und-firewall/) (<https://www.ebas.ch/2-ueberwachen-mit-virenschutz-und-firewall/>) unserer [«5 Schritte für Ihre digitale Sicherheit»](https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) (<https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/>) nachlesen. Dort finden Sie auch eine Liste von zum Teil kostenlosen Antivirenprogrammen. Sollte trotzdem dringender Verdacht einer Infektion bestehen, gilt es, richtig zu reagieren.

## Wichtigste Schritte nach einer Malwareinfektion:

1. [Ruhe bewahren, Internetverbindung trennen und letzte Datensicherung überprüfen. \(#step1\)](#)
2. [Entscheiden, ob ein Spezialist benötigt wird. \(#step2\)](#)
3. [Malware identifizieren und entfernen. \(#step3\)](#)
4. [Letzter Ausweg: Neuinstallation. \(#step4\)](#)

Der Begriff Malware setzt sich aus den englischen Begriffen «malicious» (böartig) und «Software» zusammen. Malware ist der Oberbegriff für Software, die schädliche Funktionen auf einem Gerät ausführt (wie z. B. Viren, Würmer, Trojaner, Ransomware).

## Weiterführende Informationen für Interessierte: Malwareinfektion – wie weiter?

### Schritt 1: Ruhe bewahren, Internetverbindung trennen und letzte Datensicherung überprüfen

Als Erstes sollte die Internetverbindung getrennt werden (LAN-Stecker ausziehen bzw. WLAN abschalten). Danach sollte abgeklärt werden, wie alt die letzte Datensicherung (Backup) ist. Es empfiehlt sich, ein zusätzliches, neues Backup auf ein anderes externes Speichermedium als das normale Backup zu erstellen.

Hinweis: Es ist möglich, dass mit dem Backup auch die Malware gesichert wird, was vorerst aber irrelevant ist.

### Schritt 2: Entscheiden ob ein Spezialist benötigt wird

Nun sollten Sie sich überlegen, ob Sie die Malware selbst entfernen können oder ob Sie einen Experten beiziehen wollen. Diverse Antivirenhersteller bieten einen speziellen Service zum Entfernen von Malware an. Dabei handelt es sich oft um Hilfe am Telefon oder «ferngesteuertes Malware entfernen». Dieser Service ist jedoch kostenpflichtig. Alternativ bieten auch diverse Computer-Fachgeschäfte einen Reparaturservice (speziell für Malwareinfektion) an.

### Schritt 3: Malware identifizieren und entfernen

Gewisse Malware kann direkt vom installierten Antivirenprogramm entfernt werden, jedoch nicht alle. Wenn die Malware mit Ihrem Antivirenprogramm nicht entfernt werden kann, empfiehlt sich die Verwendung eines sogenannten «Second Opinion Virenschenners», wie beispielsweise:

- [Malwarebytes \(https://de.malwarebytes.com\)](https://de.malwarebytes.com)
- [HitMan Pro \(https://www.hitmanpro.com\)](https://www.hitmanpro.com)

Falls das auch nicht hilft, muss die Malware genau identifiziert werden. Am besten nehmen Sie die Bezeichnung der Malware (welche vom Antivirenprogramm angezeigt wird) und recherchieren im Internet (von einem anderen nicht infizierten Gerät aus) nach Anleitungen, wie man diese Malware entfernen kann. Die meisten Antivirenhersteller stellen Malwaredatenbanken zur Verfügung, welche Informationen zum Entfernen bereitstellen. Wenn von Ihrem Antivirenhersteller eine Boot-CD zur Verfügung steht, sollten Sie versuchen, den Computer mit dieser CD zu starten und die Malware zu entfernen.

#### Malwaredatenbanken

- [Avira \(https://www.avira.com/de/support-virus-lab\)](https://www.avira.com/de/support-virus-lab)
- [Microsoft \(https://www.microsoft.com/security/portal/\)](https://www.microsoft.com/security/portal/)
- [Broadcom-Symantec \(https://www.broadcom.com/support/security-center/a-z\)](https://www.broadcom.com/support/security-center/a-z)
- [Trend Micro \(https://www.trendmicro.com/vinfo/de/threat-encyclopedia/\)](https://www.trendmicro.com/vinfo/de/threat-encyclopedia/)

#### Removal-Tools

- [Microsoft \(https://support.microsoft.com/en-us/help/890830/remove-specific-prevalent-malware-with-windows-malicious-software-remo\)](https://support.microsoft.com/en-us/help/890830/remove-specific-prevalent-malware-with-windows-malicious-software-remo)

- [Norton-Symantec \(https://support.norton.com/sp/en/us/home/current/solutions/kb20100824120155EN\)](https://support.norton.com/sp/en/us/home/current/solutions/kb20100824120155EN)

Für sehr verbreitete Malware stellen Antivirenhersteller sogenannte Removal-Tools kostenlos zur Verfügung. Diese überprüfen einen Computer auf bestimmte Malware und entfernt diese automatisch. Beim Herunterladen eines Removal-Tools müssen Sie unbedingt darauf achten, dass dieses von einer seriösen Webseite (z. B. eines bekannten Antivirenherstellers) stammt – es gibt Antivirenprogramme und Removal-Tools, welche von Cyberkriminellen erstellt werden und selbst Malware enthalten.

#### **Schritt 4: Letzter Ausweg - Neuinstallation**

Wenn alle diese Massnahmen nicht zum gewünschten Erfolg führen, muss der Computer von Grund auf neu installiert werden (oder Sie springen zum Schritt 2 zurück und holen sich Rat bei einem Experten).