

Die Wölfe im Schafspelz: So erkennen Sie die Antiviren- und Antispy-Betrüger

Gehen Sie den Betrügern nicht in die Falle! Im Internet werden rund 200 Sicherheitsanwendungen beworben, die angeblich kostenlose Schutzprogramme gegen Viren oder Spyware sein sollen, in Wirklichkeit aber nur ein übler Trick sind, um Sie mit falschen Warnungen zum Kauf von Reparatur- und Schutzprogrammen zu bewegen. Einige davon haben sogar Schadfunktionen und starten zum Beispiel laufend Ihren PC neu oder löschen wichtige Systemprogramme, um Sie zu erpressen. Erst wenn Sie zahlen, soll Ihr PC wieder funktionieren. Wie Sie diese Programme erkennen oder sie im Notfall beseitigen, erfahren Sie in diesem Beitrag.

Michael-Alexander Beisecker

Wie Betrügerprogramme auf Ihren PC gelangen und wie Sie das vermeiden

Im Internet lauern viele Gefahren wie Viren, Spyware oder Phishing, und es gibt daher auch Dutzende von Schutzprogrammen gegen diese Schädlinge. Doch Vorsicht: Installieren Sie keine „Schutzprogramme“, die wir Ihnen nicht empfohlen haben. Die Gefahr ist zu groß, dass Sie eine der rund 200 im Internet angebotenen betrügerischen „Sicherheitsanwendungen“ auf Ihrem PC installieren.

◀ **Installieren Sie keine unbekanntes „Schutzprogramme“**

Ein solches Programm ist meist kostenlos erhältlich, versucht Sie aber dann mit falschen Virenmeldungen oder übertriebenen Spyware-Meldungen zum Kauf der teuren „Vollversion“ zu bewegen. Viel schlimmer ist aber, dass einige dieser Programme sogar wichtige Windows-Komponenten wie die Datei „command.com“ löschen oder Windows-Funktionen deaktivieren und Windows alle paar Stunden herunterfahren.

◀ **Betrügerprogramme erpressen mit falschen Virenwarnungen**



Sieht aus wie eine Warnung von Windows, ist aber ein gemeiner Trick einer betrügerischen Anwendung: Eine gefälschte Sicherheitswarnung in Aktion

Durch Schadfunktionen werden Viren vorgetäuscht ▶ Durch die Schadfunktionen versuchen die Programme, ihre Virenmeldungen plausibler zu machen. Sie werden dann aufgefordert, die Vollversion zu kaufen, damit eine Reparatur durchgeführt werden kann. Gehen Sie darauf nicht ein, wird das Programm mit seiner Erpressung immer deutlicher und drängender.

Die Fälschungen kosten Sie Geld und öffnen Viren die Tür ▶ Einige dieser Programme sehen echten Schutzprogrammen zum Verwechseln ähnlich und erscheinen durch die falschen Meldungen auch wirksam. Doch das ist trügerisch, denn während Sie auf den Schutz vertrauen, können echte Schädlinge unerkannt auf Ihren PC gelangen. Fallen Sie auf solche Programme herein und kaufen die Vollversion, geben Sie also nicht nur nutzlos Geld aus, sondern gefährden dadurch auch die Sicherheit Ihres PC-Systems.



Sieht aus wie ein leistungsfähiges Antivirenprogramm, meldet Ihnen auch angebliche Schadprogramme, schützt aber so gut wie gar nicht vor Viren

Teilweise gelangen die Betrügerprogramme aber auch über andere Software auf Ihren Rechner. Sie sollten daher auch keine kostenlosen Programme aus dem Internet installieren, die Sie nicht genau kennen. Auch hier sollten Sie am besten nur solche Software installieren, die wir Ihnen empfohlen haben.

◀ **Ungefragte Installation über kostenlose Programme**

Doch selbst bei großer Vorsicht besteht noch die Gefahr, hereingelegt zu werden, denn die Betrüger verwenden Fenster, die wie das Windows-Update aussehen. Oder Sie erhalten einen Codec angeboten, in dem sich ein Trojaner versteckt, der anschließend ein Betrügerprogramm herunterlädt und installiert.

◀ **Gemeine Tricks: Programme sehen aus wie Updates oder Codecs**

Bestenfalls hart am Rande der Legalität sind auch Webseiten wie www.entfernen-spyware.de, die kostenlose Lösungen gegen diverse Spyware und Betrugsprogramme versprechen, aber in Wirklichkeit die Demoverision einer Antispyware liefern. Hilfe gibt es (wenn überhaupt) erst nach Kauf der Vollversion. Dabei wird verschleiert, wer dahintersteckt. Denn auf solchen Webseiten fehlt das gesetzlich vorgeschriebene Impressum mit Angabe des Verantwortlichen. Über die Registrierungsstelle der Domain können Sie aber trotzdem herausfinden, wer hinter der Webseite steckt. Bei Domains mit der Endung .de ermitteln Sie den Domaininhaber über die DENIC (www.denic.de).

◀ **Webseiten versprechen kostenlose Hilfe, liefern aber nur eine Demoverision**



Scheinbar eine Webseite mit kostenlosen Programmen zum Schutz vor Schadprogrammen, in Wirklichkeit eine getarnte Werbeseite der amerikanischen Firma Enigma, um Kunden für das Programm SpyHunter zu interessieren

Echte Schutzprogramme erkennen viele der Betrüger ► Haben Sie ein leistungsfähiges Antivirenprogramm wie „G-DATA Internet Security“ oder die „Kaspersky Security Suite“ installiert, brauchen Sie im Normalfall kein zusätzliches Schutzprogramm. Versucht sich ein Betrügerprogramm über einen Trojaner auf Ihren Rechner zu schleichen, werden Sie davor in den meisten Fällen gewarnt.

Checkliste zur Prüfung von Sicherheitsanwendungen ► Scheuen Sie die Kosten einer solchen Lösung und möchten sich mit kostenlosen Programmen schützen, dann prüfen Sie vor der Installation eines Sicherheitsprogramms mit der folgenden Checkliste, ob ein Verdacht auf eine betrügerische Sicherheitsanwendung besteht. Sie sind sicher, wenn Sie keine der folgenden Fragen mit Nein beantworten:

- Wurde das Programm vom PC-Anwender-Handbuch empfohlen?
 ja nein (Vorsicht!)
- Gibt es die Webseite des Herstellers und das Programm selbst in deutscher Sprache?
 ja nein (Vorsicht!)
- Stammt das Programm von einer der bekannten Sicherheitsfirmen wie AVG, Avira, F-Prot, G-DATA, Panda, Kaspersky, Symantec oder Trend-Micro?
 ja nein (Vorsicht!)
- Gibt es auf der Webseite ein Impressum mit den kompletten Kontaktdaten des Verantwortlichen?
 ja nein (Nicht installieren, hier liegt nahezu immer ein Betrugsversuch vor!)
- Ist im Impressum ein Unternehmen in Ihrem Heimatland eingetragen?
 ja nein (Forderungen gegen das Unternehmen sind schon aus Kostengründen kaum realisierbar, daher ist eine Anwendung der Software sorgfältig zu erwägen)

- Haben Sie den Programmnamen mit unserer Liste ab Seite B 155/08 verglichen und ist der Name nicht aufgeführt?
 ja nein
- Wird sofort deutlich auf den Preis des Programms hingewiesen?
 ja nein (Vorsicht bei angeblich kostenlosen Sicherheitsprogrammen!)

Einen gewissen Schutz bietet auch die Warnung vor gefährlichen Webseiten, wenn Sie zum Surfen im Internet als Browser den Internet Explorer 7 oder den neuen Mozilla Firefox 3 verwenden und die Funktion zum Erkennen gefährlicher Phishing-Webseiten aktiviert haben.

◀ **Warnung vor gefährlichen Webseiten**

Bitte beachten Sie auch, dass unsere Liste ab Seite B 155/08 zwar die derzeit umfangreichste Sammlung von Namen betrügerischer Sicherheitsanwendungen ist, jedoch die Hersteller ständig neue Namen, Schreibweisen und Versionen erfinden. So wurde etwa WinAntiVirusPro 2006 zuvor als WinAntiVirus 2005 angeboten. Es kann also jederzeit zum Beispiel eine Version WinAntiVirusPro 2008 auftauchen.

◀ **Achten Sie auf Namensvariationen**

Misstrauen Sie auch allen ähnlich klingenden Programmnamen, insbesondere wenn diese die martialischen Bestandteile Armor (Rüstung), Assassin (Auftragsmörder), Blaster, Crusher, Destroyer oder Demolisher (Zerstörer), Hitman (bekanntes Spiel mit einem Auftragsmörder), Killer oder Terminator enthalten. Die Autoren der Betrugsprogramme bevorzugen solche Begriffe bei der Namenswahl.

◀ **„Killer-Programme“ sind verdächtig**

Wenn Sie doch hereingefallen sind: Betrüger-programme erkennen und entfernen

Leider kann es auch bei aller Vorsicht passieren, dass Sie aus Versehen eine der betrügerischen Sicherheitsanwendungen installieren. Das fällt meistens dadurch auf, dass

◀ **Laufende Warnungen verdächtig**

laufend Warnungen vor Viren und Spyware auftreten, obwohl ein leistungsfähiges Antivirenprogramm und eine Firewall installiert sind.

- Betrugsprogramme verlangsamen den PC und führen zu Fehlern** ▶ Dazu kann Ihr PC durch ein Betrugsprogramm plötzlich deutlich langsamer laufen, und es können Fehler auftreten wie plötzliche Neustarts oder dass Windows fehlende Dateien meldet. Dann sollten Sie prüfen, ob eines der Programme aus der Liste ab Seite B 155/08 installiert ist.
- Liste der installierten Software einsehen und Betrüger deinstallieren** ▶ Dazu öffnen Sie die *Systemsteuerung*, klicken auf *Software* und vergleichen die Liste der installierten Software mit der Liste der Betrügerprogramme in diesem Beitrag. Finden Sie ein Betrügerprogramm, deinstallieren Sie es direkt mit *Software*. Die meisten dieser Programme werden dadurch tatsächlich entfernt.
- Zur Sicherheit mit mehreren Antispyware-Programmen scannen** ▶ Einige der Betrügerprogramme sind jedoch auf diese Weise nicht vollständig zu entfernen. Teilweise bleiben zusätzlich installierte Schadprogramme zurück, oder die Programme installieren sich über verborgene Automatismen wieder neu. Daher sollten Sie Ihren PC bei einem Verdacht auf Betrügerprogramme oder Spyware immer zusätzlich mit mehreren Antispyware-Programmen scannen. Ein Scan mit nur einem Programm ist zu unsicher, da die Scan-Programme bestenfalls rund 70 Prozent der im Internet kursierenden Schadprogramme erkennen. Eine Übersicht der derzeit empfehlenswerten Programme finden Sie in der nachfolgenden Tabelle:

Programm	Webseite
Ad-Aware 2007 free	www.lavasoft.de/products/ad_aware_free.php
a-squared free	www.emsisoft.de/de/software/free/
Crap Cleaner (CCleaner)	www.ccleaner.de/
SpyBot Search&Destroy	www.safer-networking.org/de/index.html

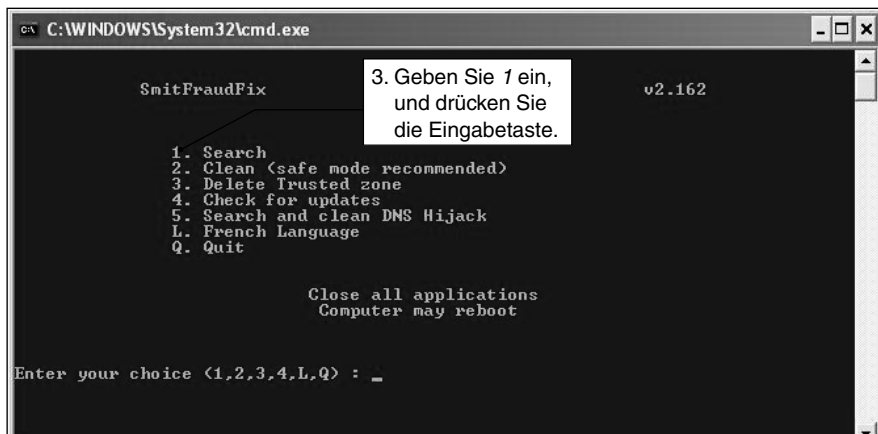
Testen Sie Ihren PC mit zumindest einem dieser vier Programme, bei bestätigtem Verdacht mit allen hier aufgeführten Programmen

Betrügerprogramme mit SmitFraudFix entfernen

Nicht alle Betrügerprogramme lassen sich mit einem der genannten Antispyware-Programme entfernen. In solchen Fällen hilft Ihnen meistens das Tool „SmitFraudFix“ weiter. Eine Liste der Programme, die Sie mit SmitFraudFix entfernen, finden Sie auf dieser Webseite: http://siri.urz.free.fr/Fix/SmitfraudFix_De.php. Das Programm wenden Sie wie folgt an:

◀ **SmitFraudFix entfernt rund 100 Härtefälle unerwünschter Programme**

1. Laden Sie die ZIP-Archivdatei mit SmitFraudFix von der Webseite <http://siri.urz.free.fr/Fix/SmitfraudFix.exe> herunter und entpacken Sie das Archiv in einem Ordner Ihrer Wahl.
2. Starten Sie „SmitfraudFix.exe“ durch einen Doppelklick.



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\System32\cmd.exe". The main window content is a black terminal with white text. At the top, it says "SmitFraudFix" on the left and "v2.162" on the right. Below this is a numbered menu:

```
1. Search
2. Clean (safe mode recommended)
3. Delete Trusted zone
4. Check for updates
5. Search and clean DNS Hijack
L. French Language
Q. Quit
```

At the bottom, it says "Enter your choice (1,2,3,4,L,Q) : _". A white callout box with a black border points to the number '3' in the menu, containing the text: "3. Geben Sie 1 ein, und drücken Sie die Eingabetaste." Below the menu, there is a warning: "Close all applications\nComputer may reboot".

SmitFraudFix ist ein DOS-Programm, mit dem Sie etwa 100 Schadprogramme von Ihrem Rechner entfernen können

4. SmitFraudFix erstellt einen Bericht in der Datei „rapport.txt“ und speichert diesen im Hauptverzeichnis Ihres Systemlaufwerks ab. Das ist meist C:\. Öffnen Sie diese Textdatei und prüfen Sie, ob SmitFraudFix ein Schadprogramm gefunden hat.

5. Starten Sie Ihren PC im abgesicherten Modus neu, indem Sie während des Starts die Taste **F8** drücken.
6. Starten Sie „SmifraudFix.exe“ erneut durch einen Doppelklick.
7. Wählen Sie diesmal Menüpunkt 2 und drücken Sie die Eingabetaste, um die infizierten Dateien zu löschen.
8. Die Frage *Do you want to clean the registry?* (Möchten Sie die Registrierungsdatenbank bereinigen?) beantworten Sie mit *Y* für „yes“ bzw. „ja“.
9. Sofern die Datei „wininet.dll“ infiziert ist, werden Sie gefragt, ob Sie diese ersetzen möchten (*Replace infected file?*). Antworten Sie auch hier mit *Y* für „yes“ bzw. „ja“.
10. Starten Sie Ihren PC neu, um den Reinigungsvorgang abzuschließen. Den Bericht über die Reinigungsaktion finden Sie wiederum in der Datei „rapport.txt“.

Übersicht der Betrügerprogramme: Haben Sie eines dieser Programme auf Ihrem Rechner?

Die 200 gefährlichen Fälschungen ▶ Prüfen Sie über *Start/Einstellungen/Systemsoftware/Software* (Windows XP) oder *Start/Systemsoftware/Software* (Windows Vista) ob Sie eines dieser rund 200 falschen Antivirenprogramme auf Ihrem Rechner installiert haben, und deinstallieren Sie es dann:

100 Percent Anti-Spyware
#1 Spyware Killer
1 Click Spy Clean
IstAntiVirus

2004 Adware Remover & Blocker
2004 Spyware Remover & Blocker
about :blank 2005
Ad Armor

AdDestroyer
AdDriller
Ad-Eliminator
Ad-Protect
AdProtector

Ad-Purge Adware & Spyware Remover
ADS Adware Remover
Ads Alert
Advanced Spyware Remover
Adware & Spyware Firewall
Adware Agent
Adware Cops
Adware Filter
Adware Finder
Adware Hitman
Adware Sheriff
AdWare SpyWare Blocker & Removal
Adware Striker
Adware/Spyware Remover
AdwareAlert
AdwareBazooka
AdwareDelete
AdwareDeluxe
AdwareHunter
Adware-Nuker
AdwarePatrol
AdwarePro
AdwarePunisher

AdwareRemover 1
AdwareRemover 2
AdwareSafe
AdwareSafety
AdwareSpy
AdwareTools
AdwareX
Ad-Where 2005
Agent Spyware
AlertSpy
AlfaCleaner
Anti Virus Pro
AntiSpy Advanced
AntiSpyware
Anti-Spyware Blocker
AntiSpyZone
AntiVermins
AntiVerminser
Antivirgear
Antivirus Email
AntiVirus Golden
AntiVirus Protector
Anti-Virus&Spyware
ArmorWall
BestGuardPlatinum
Botsquash

BPS Spyware & Adware Remover
Brave Sentry
CheckFlow
CheckSpy & Anti Spyware 2005
Clean Space
CoffeeCup Spyware Remover
Consumer Identity
CurePCSolution
CyberDefender
Defenza
Doctor Adware
Doctor Adware Pro
DriveCleaner 2006 Free
Easy Erase Spyware Remover
Easy SpyRemover
Easy Spyware Killer
Elimiware
Emco Malware Bouncer
Errorsafe
ETD Security Scanner
ExpertAntiVirus
Flobo Free Anti Spyware Clean
Freeze.com

Froggie Scan
GarbageClean
GoodbyeSpy
GuardBar
HitVirus
IC Spyware Scanner
Intelligent Spyware Cleaner
Internet Cleanup
InternetAntiSpy
iSpyKiller
JC Spyware Remover & Adware Killer
KaZaaP
KillAllSpyware
KillAndClean
KillSpy
MalwareAlarm
MalwareScanner
MalwareWipe
MalwareWiped
MalwareWiper
MalWhere
Max Privacy
MaxNetShield
MicroAntivirus

MNS Spyware Remover & History Eraser
MyNetProtector
MyPCTuneUp
MySpyFreePC
MySpyProtector
NetSpyProtector
No-Spy
NoSpyX
One-Shot Antivirus
PAL Emergency Response
PAL Spyware Remover
PC AdWare SpyWare Removal
PC Health Plan
PCArmor
pcOrion
PestBot
Pestcapture
PestProtector
PestTrap
PestWipeR
Privacy Champion
Privacy Crusader
Privacy Defender
Privacy Tools 2004

Protect Your Identity
Protector
PSGuard
PurityScan
PuritySweep
QuickCleaner
Race Spyware
Real AdwareRemoverGold
RegFreeze
Registry_Doctor
RemidyAntiSpy
RemoveIT Pro
Rosecitysoftware
Safe & Clean
SafeWebSurfer
SamuraiSpy
Scan & Clean
Scan & Repair Utilities 2006
ScanSpyware
Scumware-Remover
SecureMyPC
Security iGuard
Securitysuite
SlimShield
SmartSecurity

Spy Annihilator
Spy Detector
Spy Reaper
Spy Snipe
Spy Sniper Pro
Spy Stalker
Spy Striker
Spy-Ad Exterminator Pro
SpyAdvanced
SpyAssassin
SpyAssault
SpyAxe
SpyBan
SpyBeware
SpyBlast
Spy-Block
SpyBouncer
SpyBrowser
SpyBurn
SpyClean
SpyCleaner
SpyContra
Spy-Control
SpyCrush
Spy-Crusher
SpyCut

SpyDawn
SpyDeface
SpyDeleter
SpyDemolisher
SpyDestroy Pro
SpyEliminator
SpyFalcon
SpyFerret
SpyFighter
SpyFirewall
SpyGuardian Pro
SpyHeal
SpyiBlock
SpyiKiller
Spyinator
Spy-Kill
SpyKiller
SpyKiller 2005
SpyKillerPro
SpyLax
SpyLocked
SpyNoMore
SpyOnThis
Spy-Out
SpyPry
SpyRemover

SpySheriff
SpyShield
SpySpotter
SpyToaster
SpyTrooper
SpyVest
SpyViper
Spyware & Adware Removal
Spyware & Pest Remover
Spyware & Pop-Up Utility
Spyware Annihilator
Spyware Blaster
Spyware Bomber
Spyware C.O.P.
Spyware Cleaner
Spyware Cleaner & Pop-Up Blocker
Spyware Cops
Spyware Defense
Spyware Destroyer
Spyware Detector
Spyware Disinfecter
Spyware Immobilizer
Spyware Medic
Spyware Protection Pro

Spyware Quake	SpywareTek	Ultimate Cleaner
Spyware Removal System	SpywareThis	Ultimate Defender
Spyware Remover	SpywareXP	UnSpyPC
Spyware Shield	SpywareZapper	VBouncer
Spyware Slayer	SpyWiper	Video ActiveX Access
Spyware Sledgehammer	StopGuard	VirusGuard
Spyware Snooper	StopItBlockIt 2005	VirusProtectPro
Spyware Stormer	Super Spyware Remover	WareOut Spyware Remover
Spyware Striker Pro	System Detective	WebSafe Spyware Secure
Spyware Suite 2005	SystemStable	Win AntiVirus Pro 2006
Spyware Terminator	TeoSoft Anti-Spyware	WinAntiSpy 2005
Spyware Vanisher	Terminexor	WinAntiSpyware 2006
Spyware Wizard	The Adware Hunter	WinAntiVirus 2005
SpywareAssassin	The SpyGuard	Wincleaner AntiSpyware
SpywareAvenger	The Spyware Detective	Winhound Spyware Remover
SpywareBeGone	The Spyware Shield	Winkeepe
SpywareCrusher	The Web Shield	WinSOS
SpywareHospital	TheSpywareKiller	WorldAntiSpy
SpywareHound	Titan AntiSpyware	X-Con Spyware Destroyer
SpywareKill	TitanShield Antispyware	Xspyware
SpywareKilla	Top10Reviews SpyScan	X-Spyware
SpywareNo!	True Sword	XSRemover
SpywareRemoval	TrueWatch	ZoneProtect AntiSpyware
Spyware-Stop	TZ Spyware Adware Remover	
SpywareStrike	UControl	

Bekannte Namen von falschen Sicherheitsprogrammen