DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Warum in Windows nicht als Adminstrator gesurft werden soll

Sie finden auf Ihrem PC nach der Einrichtung von PC-Blitzhelfer ein zweites Benutzerkonto mit Namen ADMINKONTO, es ist ohne Passwort eingerichtet. Empfehlung: der Standard-Benutzer (in der Regel der Vorname des Besitzers) sollte nur mit eingeschränkten Rechten arbeiten.

Also das normale Tagesgeschäft (Surfen, Briefe schreiben, Emails lesen usw.) sollte nur als normaler Hauptbenutzer erledigt werden.

Warum gibt es diese Empfehlung?

Hier nun verschiedene Erklärungen zum Thema:

Windows stellt verschiedene Arten von Benutzerkonten zur Verfügung. ***Das standardmäßig eingerichteten Administratorkonto sollten Sie für den Alltagseinsatz nicht benutzen, stattdessen richten Sie für sich und andere PC-Benutzer geeignete Benutzerkonten mit eingeschränkten Rechten ein, um Malware und Hackern von vornherein den Zugriff zu erschweren.***
Eine kluge Benutzerverwaltung hat aber noch mehr Vorteile: Sie können den PC für mehrere Anwender einrichten und jedem ein Konto mit seinen persönlichen Daten und Einstellungen zuteilen.
Sicher, stabil, ordentlich
Ein Betriebssystem ist sehr empfindlich. Das Verschieben, Löschen oder Überschreiben der falschen Datei kann alles lahmlegen. Darum wurde schon vor Jahren das Konzept der Benutzerrechte eingeführt: ***Heikle Arbeiten wie Programme installieren, Systemdateien verwalten oder die Festplatte formatieren sollte nicht jeder Benutzer ausführen. Dazu ist ein spezielles Administratorkonto vorgesehen, mit dem man auf alle Systembereiche vollen Schreibzugriff hat.***
Für alltägliche Tätigkeiten wie surfen, mailen, schreiben, Bilder bearbeiten, Musik hören etc. braucht der Anwender hingegen keinen Schreibzugriff in die System- und Programmordner. Es reicht, wenn er alle Anwendungen starten und seine Dateien in persönlichen Ordnern ablegen kann. Auch individuelle Einstellungen wie das Aussehen der Symbolleisten oder die Fenstergröße der einzelnen Programme sind in einem Standardkonto problemlos möglich.
Halten Sie sich an diese Aufteilung, haben Sie drei entscheidende Vorteile: mehr Sicherheit, ein stabileres System und eine bessere Ordnung.

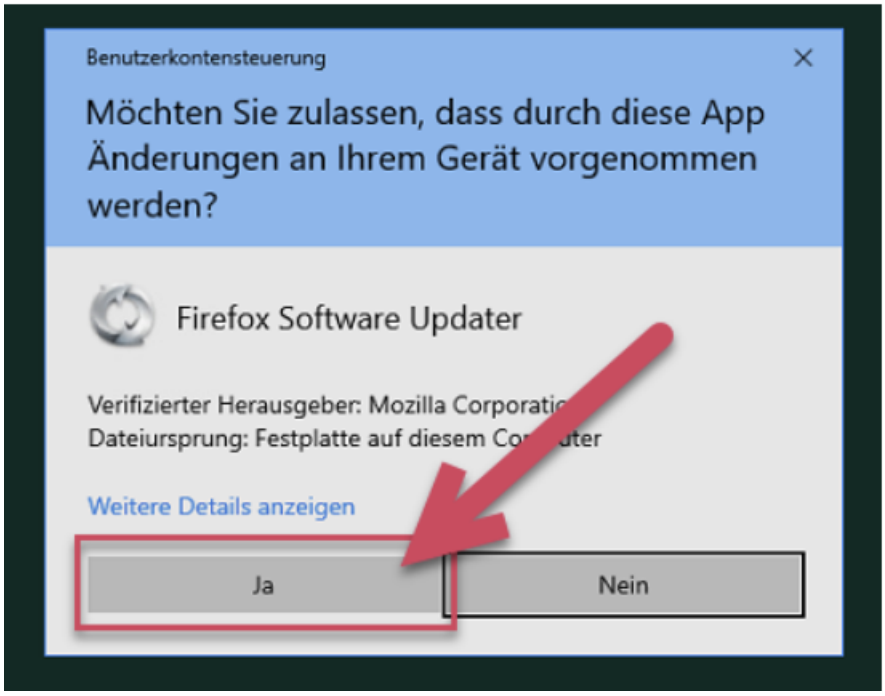
Quelle: https://www.pcwelt.de/ratgeber/Windows-Sicherheit-Administrator-und-Benutzerkonten-unter-Windows-58685.html

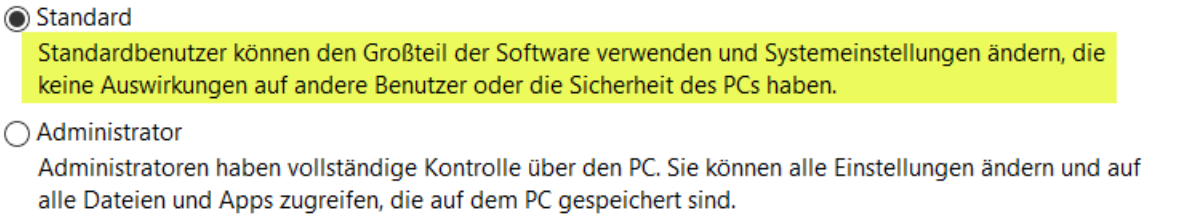
---

Für tiefgehende Änderungen am System sind Administratorenrechte erforderlich. Ohne diese Rechte können zahlreiche Schädlinge nicht Fuß fassen. Deshalb ist es eine der effektivsten Schutzmaßnahmen, als Administrator bzw. als Nutzer mit Administratorrechten nicht zu surfen und vor allem keine E-Mails zu empfangen. Richten Sie einen „Standardbenutzer“ ein und nutzen Sie Administratorenkonten nur, wenn es unumgänglich ist!

In der Systemsteuerung finden Sie die „Benutzersteuerung“ bzw. „Benutzersteuerung und Jugendschutz“. Dort können Sie ein „Benutzerkonto hinzufügen“. Wenn Sie ein „Neues Konto erstellen“, wählen Sie „Standardbenutzer“ als Kontotyp. Benutzen Sie zukünftig diese Konto als Hauptkonto. Seit Windows Vista können Sie auch als Standardbenutzer fast alle Tätigkeiten durchführen, für die ein Administratorkonto nötig wäre. Sie werden einfach von Windows nach dem Administrator-Passwort gefragt und zeitweilig zum Administrator „hochgestuft“. Vergessen Sie nicht, dem Administratorkonto ein Passwort zu geben.

Quelle: https://de.wikibooks.org/wiki/Internet:_Sicherheit:_Administratorrechte





Hier ist die Erklärung zur UAC

Die **Benutzerkontensteuerung** (auch englisch *User Account Control*, UAC) ist ein im Betriebssystem Windows von Microsoft integrierter Sicherheitsmechanismus, welcher mit Windows Vista eingeführt wurde. Ziel der Benutzerkontensteuerung ist es, die Sicherheit des Systems zu verbessern, indem Software zunächst nur mit einfachen Nutzerrechten ausgeführt wird anstatt mit Administratorrechten. Administratoren können eine Erhöhung der Rechte veranlassen, sollte die Anwendung diese benötigen. Die Benutzerkontensteuerung wurde eingeführt, da viele Anwender mit Administratorprivilegien arbeiten, welche bis inklusive Windows XP direkt auf gestartete Anwendungen übertragen wurden. Dieses Verhalten stellte ein großes Sicherheitsrisiko dar, weil auch etwaige Schadsoftware administrative Rechte erhielt.

Wenn sich mit aktiver UAC ein Administrator am System anmeldet, so arbeiten von ihm gestartete Programme dennoch zunächst nur mit den Rechten eines normalen Benutzers. Sobald eine Anwendung administrative Berechtigungen für ihre Ausführung anfordert, wird ein Dialogfeld angezeigt, welches explizit zu bestätigen ist, um die Rechte zu gewähren.

Quelle: https://de.wikipedia.org/wiki/Benutzerkontensteuerung

Wann die UAC „zuschlägt“ weiss so richtig im Voraus keiner, eben dann wenn Microsoft meint diese Aktion sei besonders schützenswert.
Sie müssen dann einfach nur 1x mehr klicken, dafür sind Sie im Gesamten sicherer unterwegs.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Benutzerkonten unter Windows

Leider ist es in der Windowswelt immer noch so, dass bei der Neuinstallation der **Benutzer standardmäßig mit Administrator-Rechten** angelegt wird. Das ist auch wichtig, da zum Ändern von Systemeinstellungen und Installationen, Administrationsrechte verlangt werden, aber…

Für das normale tägliche Arbeiten am Computer, sollte man aus Sicherheitsgründen **eingeschränkte Benutzerrechte** definieren. Mit diesen eingeschränkten Rechten ist es z.B. nicht mehr möglich Dateien anderer Benutzer auf dem Rechner zu lesen und zu ändern, bzw. im Windowsordner und Programmordner zu schreiben. Sollte es dennoch versucht werden, bekommt der User eine Fehlermeldung. Das Anlegen **eingeschränkter Benutzer** hat seine Vor- und Nachteile. An einigen Stellen hat der Benutzer zu wenig Rechte und an anderer Stelle wieder zu viele.

So verhält sich das auch beim Surfen im Internet. Sollte man sich mit gefährlichen Viren infizieren, haben diese keine Rechte sich zu installieren und können keinen Schaden am System anrichten. Sollte im Fall der Fälle dann doch der Rechner mit Malware infiziert werden, beschränkt sich die Infizierung in der Regel nur auf das **eingeschränkte Konto** und kann über das **Administratorkonto gelöscht bzw. bereinigt** werden.

Da ein Administrator "alles" darf, auch wichtige Systemdateien verändern - geht es einem Virus oder Spyware genauso: Wenn ein Schädling mit Administrator Rechten auf einen PC gelangt, kann er sich ungehindert ausbreiten oder Windows-System-Dateien manipulieren um zum Beispiel Hintertüren zu öffnen.

Wenn Ihr hingegen mit eingeschränkten Rechten surft, hat auch ein eventueller Schädling nur eingeschränkte Rechte. Das bedeutet er kann nichts auf C:, also nichts an dem Windows-Betriebssystem verändern. Er kann im schlimmsten Fall lediglich das Benutzerkonto infizieren. Durch Löschen des Kontos wäre auch der Virus wieder gelöscht. Bei einem Virus hingegen der Windows verändert hat, muss meistens die Festplatte formatiert, und anschließend Windows neu installiert werden.

Viele Viren lassen sich ohne Administrator-Rechte erst gar nicht installieren. Daher bringt dieser Schritt mit den eingeschränkten Rechten eine sehr gut erhöhte PC-Sicherheit.

Ich empfehle unter Windows 7, 8 und 10 die Nutzung des Schutzes der UAC, innerhalb eines Administrator-Konto:

Seit Windows Vista/7/8/10 wurde die neue Funktion der Benutzerkontensteuerung UAC (User Account Control) eingeführt. Wenn diese eingeschaltet ist, wird der PC gut geschützt ohne dass der Nutzer auf den Komfort des Administrator-Modus verzichten muss.

Durch die UAC ist man standardmäßig auch in einem Administrator Konto zunächst mit eingeschränkten Rechten unterwegs. Die UAC bleibt im Hintergrund immer aktiv und kontrolliert welche Dinge der Benutzer macht und welche Aktionen die Programme vornehmen. Solange der Benutzer und die Programme nichts an Windows verändern, meldet sich die UAC auch nicht. Aber sobald "jemand" an Windows etwas verändern möchte, fragt die UAC den Benutzer:

Möchten Sie zulassen, dass durch das folgende Programm Änderungen an diesem Computer vorgenommen werden?

Diese Frage solltet Ihr Euch gut merken, denn wenn Ihr jetzt auf Ja klickt, arbeitet das Programm als Administrator weiter, und kann beliebig Änderungen an Windows vornehmen. Wenn es nun ein Virus wäre, könnte dieser jetzt den ganzen Computer lahm legen.

Wenn Ihr bei dieser Frage hingegen auf Nein klickt, verweigert Windows den weiteren Zugriff und das Programm kann keine Änderungen an Windows vornehmen. Ein Virus könnte damit keinen Schaden anrichten. (Genauso wie der Zugriff auch in einem klassischen eingeschränkten Benutzerkonto verweigert worden wäre)

Daher klickt, wenn Ihr im Internet am Surfen seid oder wenn Ihr Emails lest, bei eventuellen UAC Nachfragen stets auf Nein. Nur wenn Ihr Euch ganz sicher seid dass es sich um eine seriöse Nachfrage handelt, (zum Beispiel weil Ihr gerade ein Programm installiert oder ein Update von Java, etc.) klickt bei UAC Nachfragen auf: Ja

Quelle: https://www.elves-castle.de/pc-sicherheit/ohne-administratorrechte-surfen.html