Tipps für einen gesunden Mac

von John Daniel auf etresoft.com/healthymac

Übersetzung und Anmerkungen von KJM

Hier sind ein paar Tipps, die ich gesammelt habe, als ich Leuten in den Apple Support Communities half.

1 Safari Pop-up-Scam

Es gibt heutzutage eine epidemisch wachsende Menge aller Arten von Scams – von Rohreinigung bis zu Wasserkochern. Dieser Tipp handelt von einem speziellen Scam: dem Safari Pop-up. Während Du im Internet blätterst, öffnet sich ein Dialog und erzählt Dir, dass:

- Du einen Preis gewonnen hast
- das FBI illegale Aktivität entdeckt hat
- Dein Computer infiziert ist
- Du irgendwelche Software herunterladen musst

Nichts davon ist wahr. Du wirst aufgefordert, eine Telefonnummer zu wählen. Das Popup-Fenster lässt sich nicht schließen. Wenn Du Safari neu startest, erscheint auch das Pop-up-Fenster wieder.

Wenn Du Deinen Mac auf OS X 10.10.4 oder neuer aktualisierst, kannst Du OK klicken oder die Return-Taste drücken (nützlich, wenn das Fenster nur teilweise auf dem Bildschirm zu sehen ist), um das Pop-up-Fenster zu schließen. Beim nächsten Mal, wenn der Dialog sich wieder öffnet, kann man ihn dann endgültig schließen. Auf älteren Systemen kann man Safari mit Force-Quit beenden *(cmd-opt-esc, Safari auswählen und „Sofort beenden")* und dann die Shift-Taste gedrückt halten, wenn man Safari neu startet *(um das erneute Öffnen des selben Fensters zu vermeiden)*.

Wichtig: Ruf die angegebene Nummer NICHT an! Die Scammer wollen die Kontrolle über Deinen Mac übernehmen, Dir kryptische, aber harmlose Log-Dateien zeigen, irgendwelche Low-Level-Änderungen mithilfe des Terminals durchführen und dafür Deine Kreditkarte mit $500 oder mehr belasten. Wenn das passiert, solltest Du:

- die Polizei anrufen
- Deine Bank anrufen und Deine Kreditkarten sperren lassen
- Schutz gegen Identitätsdiebstahl kaufen
- Deinen Mac auf einen Zustand vor dieser Attacke zurücksetzen und
- all Deine Passwörter auf Deinem Mac, Deinen eMail- und Internet-Konten ändern

2 Computer-Sicherheit

Die wichtigste Sicherheits-Funktion auf dem Mac ist **Gatekeeper**. Geh in Systemeinstellungen > Sicherheit > Allgemein und vergewissere Dich, dass bei „Apps-Downloads erlauben von …" folgendes eingestellt ist: „Mac App Store und verifizierte Entwickler". Selbst mit dieser Einstellung musst Du immer noch jede Installation von Software, die aus dem Internet heruntergeladen wird, bestätigen. Es ist immer eine sichere Wahl, den „Abbrechen"-Button zu klicken.

Als nächstes geh zu Systemeinstellungen > **Freigaben** und vergewissere Dich, dass dort alle Freigabe-Dienste ausgeschaltet sind. Wenn Du sie wirklich brauchst, kannst Du sie aktivieren, wenn Du zuhause bist, aber sie sollten immer abgeschaltet sein, wenn Du Dich in der Öffentlichkeit aufhältst z. B. in einer Bücherei, Schule, Internetcafé.

Wichtig: Eine Firewall wird Dich nicht schützen, wenn eine Freigabe aktiviert ist. Firewalls sind Werkzeuge für Netzwerk-Administratoren. Die Firewall auf Deinem Mac ist ein Marketing-Gimmick. Wenn Du Sicherheits-Sorgen hast, lass alle Freigabe-Dienste ausgeschaltet. Verlass Dich nicht auf die Firewall. Sie tut nicht das, was Du denkst.
Andere Pop-up-Dialoge: Von Zeit zu Zeit kann der Mac andere Arten von Pop-ups anzeigen, die dazu auffordern, Software zu installieren oder Dein Passwort anzugeben. Auch hier ist ein Klick auf „Abbrechen" immer die sichere Wahl. Wenn Du ein Flash-Update installieren musst, geh direkt auf die Adobe-Website und lade das Update dort herunter.

3 Adware

Eine andere moderne Mac-Seuche ist Adware. Ich empfehle AdBlock, um die meisten Werbe-Anzeigen zu blockieren. Wenn Du denkst, dass Du bereits irgendwelche Adware installiert hast, dann ist der einzige sichere Weg, sie zu entfernen, AdwareMedic *(jetzt: **Malwarebytes Anti-Malware for Mac**)*.

4 Dein Mac braucht keine Säuberungssoftware.

Er wird umso besser laufen, je weniger Du daran herumfummelst.

5 Malware, Trojaner, Viren

Obwohl es diese Menge an Scams und Adware für den Mac gibt, ist echte Schadsoftware wie Trojaner und Viren immer noch extrem selten. Du brauchst tatsächlich keine Antivirussoftware auf einem Mac. Die meisten Antivirus Programme suchen auf Deinem Mac nach Windows-Malware, die für Dich harmlos ist. Dafür wird sie Deinem Mac langsamer machen und kann Probleme verursachen. Apple hat einen effektiveren Malware-Scanner in OS X eingebaut als Du ihn sonstwo finden kannst.

6 Halte Deinen Mac aktuell

Es ist wichtig, Deinen Mac auf aktuellem Stand zu halten. Für ältere Versionen des Betriebssystems bietet Apple keine Sicherheits-Updates mehr an. Wenn Du irgendwelche System-Modifikationen installiert hast, dann solltest Du **EtreCheck** laufen lassen, um herauszufinden, welche das sind, und um Dich zu vergewissern, dass sie auch auf dem neuen System laufen werden, bevor Du das System-Update durchführst. Diese Programme werden aufgelistet unter Kernel Extensions, Launch Daemons, Launch Agents und User Launch Agents. Alles, was unter Startup Items aufgelistet ist, wird definitiv nicht unter OS X 10.10 „Yosemite" laufen und sollte aktualisiert werden.

7 Mac-Upgrades

Bevor Du die Software Deines Macs aktualisierst, ist es auch wichtig, Dich zu vergewissern, dass Dein Mac tatsächlich in der Lage ist, die neueste Version des Betriebssystems zu verwenden. Aktuelle Versionen von OS X sind meist langsamer und stellen höhere Anforderungen als noch vor ein paar Jahren. Man braucht zusätzlichen Arbeitsspeicher und vielleicht ein SSD Upgrade. Dein **EtreCheck**-Bericht wird Dir zeigen, ob der Arbeitsspeicher Deines Macs sich erweitern lässt. Abgesehen von iMacs, kann jeder Mac mit erweiterterem RAM auch auf SSD aufgerüstet werden.

8 Backups

Backups sind lebenswichtig. Alle Mac-Anwender sollten Time Machine benutzen. Andere Arten von Backups können in bestimmten Situationen nützlich sein, aber Time Machine sollte Dein Haupt-Backup sein.

9 Software installieren

Alle Mac-Anwender sollten möglichst immer den Mac App Store benutzen. Apps aus dem Mac App Store werden regelmäßig aktualisiert, von Apple auf Qualität und Sicherheit geprüft, und sind auf einfache Weise wieder zu entfernen. Bevor Du Software aus anderen Quellen installierst, vergewissere Dich, dass Du weißt, wie Du sie wieder entfernen kannst. Ich empfehle sehr, die originalen Installations-Dateien aufzubewahren, da sie oft auch Uninstaller oder zumindest Anleitungen zum Deinstallieren enthalten.

Wichtig: Jede Software, die einen eigenen Installer benutzt und zum Eingeben des Admin-Passwortes auffordert, kann schwierig zu deinstallieren sein.

10 Software entfernen

Um Software zu entfernen, die aus dem Mac App Store geladen wurde, geht man einfach ins LaunchPad, findet das Icon der Software, klickt darauf und hält die Maustaste gedrückt. Das Icon beginnt, sich zu schütteln, und ein X-Button erscheint in der oberen linken Ecke. Klick auf das X, um die App zu deinstallieren.

Wenn Du Software aus anderen Quellen installiert hast, ist der einzig sichere Weg zum Entfernen der Software ein vom Hersteller mitgelieferter Uninstaller oder entsprechende Anleitungen zum Deinstallieren. Benutze nie einen „App-Zapper". Versuch nie, eigenhändig Dateien aus verborgenen Verzeichnissen zu löschen. Mache Apps können sich selbst deinstallieren. Wenn Du eine App teilweise gelöscht hast, kann es sein, dass Du sie erst wieder neu installieren musst, bevor die interne Deinstallations-Prozedur korrekt ablaufen kann.

11 Hilfe bekommen

Wenn Du weitere Hilfe benötigst, schlage ich vor, Du kontaktierst den Apple Support direkt oder einen Apple Authorized Service Provider. Es gibt eine Menge schlechter Ratschläge im Internet und auch einige gute Tipps, aber es kann schwierig sein, den Unterschied zu erkennen. Selbst gute Ratschläge von vor ein paar Jahren könnten heute Deinen Mac beschädigen.

Unglücklicherweise kann ich die Apple Support Communities nicht länger als eine verlässliche Quelle für Hilfe empfehlen. Apple benutzt eine „Gamification strategy" für die Website, indem es ein „Points/Reputation"-System eingeführt hat. Solche Systeme können unterhaltsam sein, sind aber auch suchterzeugend. Einige Teilnehmer spielen sehr erfolgreich mit diesem System. Die Scams und Risiken, vor denen ich warne, werden in den Apple Support Communities aktiv praktiziert. Von den hier aufgelisteten Ratschläge wird dort aktiv abgeraten. Auf viele Weisen haben die Apple Support Communities begonnen, ein massiver Tech Support Scam zu werden, in dem die Währung Punkte sind statt Geld.

*Anmerkungen von KJM: Ich empfehle Thomas Reed's Adware Medic (jetzt „**Malwarebytes AntiMalware for Mac**") und ich schätze John Daniel's **EtreCheck** sehr, aber ich gebe ihm nicht in jeder scharfen Formulierung Recht. Man kann nicht immer sicherheitshalber auf „Cancel" klicken. Bei mancher Software-Installation wie z. B. LibreOffice führt kein Weg daran vorbei: man muss zur ersten Inbetriebnahme Apple's Gatekeeper zeitweilig deaktivieren. Aktuell kann Default Folder X 4 unter El Capitan nur benutzt werden, wenn die neue Sicherheitsfunktion SIP deaktiviert wird – und dann ist man auch nicht unsicherer als zuvor unter OS X Yosemite. — Mit Uninstaller-Programmen wie App-Cleaner oder AppDelete habe ich persönlich bislang nur gute Erfahrungen gemacht. Gute Uninstaller richten sich in erster Linie nach den Installationsquittungen der Programme. Sind die vorhanden, ist das Löschen der Programm-Komponenten kein Problem. Zugehörige Einstellungsdateien werden zuverlässig gefunden und entfernt. — Zum Erkennen (zwecks Löschen) von Apps aus Mac App Store reicht es, im LauchPad die Optionstaste zu drücken.*