PC-Schutz: 10 Maßnahmen für mehr Sicherheit

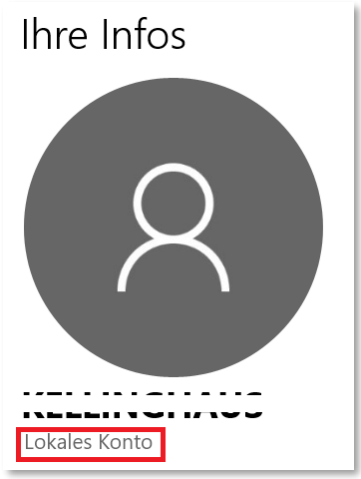
1. Nutzen Sie nur ein eingeschränktes Benutzerkonto und melden Sie sich nicht immer als Admin an.

Was ist ein Admin –Benutzerkonto? Wo liegt der Unterschied zwischen einem eingeschränkten Benutzerkonto und einem Admin-Konto?

Administratorkonto		**Eingeschränktes Benutzerkonto**
• Das Administratorkonto verfügt über den **uneingeschränkten Zugriff** auf das installierte Betriebssystem. • Das Administratorkonto kann auch zu **erheblichen Sicherheitsrisiken** führen, da es einen **Vollzugriff** auf alle relevanten Systemdateien ermöglicht.		• Für jeden Benutzer wird ein eigenes Benutzerkonto angelegt, unter dem er zukünftig alle seine Dateien und Dokumente finden kann. • Dadurch arbeitet jeder Benutzer eines Betriebssystems in seinem geschlossenen Benutzerkonto und kann somit die Daten anderer Benutzer nicht verändern oder löschen. Andere Benutzer haben keinen Zugriff auf dessen Daten. • Einzig der Administrator des Systems hat den kompletten Zugriff auf alle Konten, Daten und Dateien.
➡ Bei der Verwendung eines eingeschränkten Benutzerkonto erhöht sich die Sicherheit aktueller Computer und Betriebssysteme erheblich und viele Schadprogramme haben keine Chance auf dem Computersystem des Anwenders zu landen, denn Viele der aktuellen Viren können nur mit den Rechten eines Administrators arbeiten und auf dem System Schäden verursachen.		

Wie erkenne ich die verschiedenen Benutzerkonto-Typen?

1. Gehe Sie auf Start
2. Wählen Sie das oberste Symbol n der linken Spalte aus.
3. Wählen Sie „Kontoeinstellung ändern“ aus.
4. Es öffnen sich ein neues Fenster mit „Ihre Infos“.



RECHENZENTRUM

Wie richtet man ein eingeschränktes Benutzerkonto (Lokales Konto) ein?

1. Wählen Sie die Schaltfläche **Start** und dann **Einstellungen** > **Konten** > **Familie & weitere Kontakte** (in manchen Windows-Editionen einfach nur **Andere Personen**) > **Diesem PC eine andere Person hinzufügen** aus.

2. Wählen Sie unten auf der Seite **Ich kenne die Anmeldeinformationen für diese Person nicht** aus, und wählen Sie dann unten auf der nächsten Seite **Benutzer ohne Microsoft-Konto hinzufügen** aus.

3. Geben Sie einen Benutzernamen, ein Kennwort und einen Kennworthinweis ein, und wählen Sie dann **Weiter** aus.

2. Halten Sie Ihr Betriebssystem (Windows) aktuell.

1. Gehen Sie auf Start
2. Gehen Sie auf Einstellungen
3. Es öffnet sich ein neues Fenster „Windows-Einstellungen“. Gehen Sie auf „Update und Sicherheit“.
4. Im Fenster „Windows Update“ kann man den aktuellen Update-Status herauslesen.
5. Um sicherzugehen, dass keine Updates fehlen, wählen Sie „Nach Updates suchen“ aus.
6. Existieren neue Update, so laden Sie diese herunter und sie werden automatisch installiert.
7. Nach der Installation könnte ein Neustart von Nöten sein.

3. Eine gute Antiviren-Software sollte für Sie Pflicht sein, um Schädlinge fern zuhalten.

- Die Universität Regensburg setzt Microsoft Defener als Antivirenschutzprogramm ein

- Weitere Information zu Sophos und deren Installation: https://www.uni-regensburg.de/rechenzentrum/serviceangebot/sicherheit/arbeitsplatzsicherheit/index.html

4. Halten Sie Ihren Browser auf den neusten Stand.

Anleitungen zu den einzelnen Browsern finden Sie hier:

Google Chrome:
https://support.google.com/chrome/answer/95414?co=GENIE.Platform%3DDesktop&hl=de

Firefox:
https://support.mozilla.org/de/kb/firefox-auf-die-letzte-version-aktualisieren

Internet Explorer: Der Support wurde am 15. Juni eingestellt.

Microsoft Edge:
https://support.microsoft.com/de-de/topic/microsoft-edge-updateeinstellungen-af8aaca2-1b69-4870-94fe-18822dbb7ef1

Opera:
https://www.opera.com/de/browsers/opera/beta

Safari:
https://support.apple.com/de-de/HT204416

5. Laden Sie Daten und Programme nur von vertrauenswürdigen Quellen herunter.

- Es ist Mitarbeitern der UR untersagt, aus fremden Quellen Software herunterzuladen.
- Gehen Sie auf Softwarekatalog und geben Sie Ihre Zugangsdaten ein:
- https://serviceportal.uni-regensburg.de/i/software/catalog
- Unser RZ berät, unterstützt und hilft bei der Auswahl, Anschaffung, Installation, bis hin zu Aktualisierung, Versionsumstellung und Deinstallation von Software.

6. Speichern Sie Daten nicht lokal auf Ihrer Festplatte ab. Nutzen Sie die File-Ordner der UR für Ihre Speicherung.

Keine weiteren Angaben.

7. Fertigen Sie regelmäßig Sicherheitskopien und Backups an.

- Wenn Sie Ihre Daten in Ihrem persönlichen File-Ordner in unseren File-Servers des RZ abspeichern, dann werden tägliche Backups von unseren RZ-Mitarbeitern übernommen.
- Darüber hinaus können Sie die von der UR angebotene „Cloud-Version“ MyFiles nutzen.

Weitere Informationen zu angebotenem Speicherplatz: https://www.uni-regensburg.de/rechenzentrum/serviceangebot/server-cloud-service/speicherplatz/index.html

8. Schließen Sie keine externen Festplatten oder USB an Ihren Rechner an.

Schadprogramme können ins UR-Netz gelangen durch USB-Sticks und externen Festplatten.

➡ Dateien sollten via File-Ordner der UR ausgetauscht werden.

9. Nutzen Sie unterschiedlich komplexe Passwörter für einzelne Logins

Siehe Handlungsempfehlung „Komplexe Passwörter“.

10. Bleiben Sie misstrauisch und halten Sie sich bei der Weitergabe persönlicher Informationen zurück.

- Niemals Zugangsdaten oder vertrauliche Informationen an Dritte weitergeben oder per Mail versenden!
- Das RZ wird sie niemals telefonisch oder per Mail nach Ihren Zugangsdaten fragen!