# VSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHEIT IVSICHERHE

#### **Passwörter**

- Achten Sie auf komplexe Passwörter ohne persönlichen Bezug (mind. acht Zeichen mit Sonderzeichen). Sichere Passwörter können Sie z. B. mit Hilfe eines Passwortgenerators erzeugen.
- Verwenden Sie unterschiedliche Passwörter für die Anmeldungen bei verschiedenen Diensten.
- > Hinterlegen Sie Ihre Passwörter an einem sicheren Ort, z. B. einem Passwortsafe.
- Geben Sie Passwörter niemals weiter und vermeiden Sie es möglichst, Ihre Passwörter auf unbekannten PCs einzugeben.
- Wenn Ihr Passwort anderen Personen bekannt geworden ist, sollten Sie es sofort ändern oder Ihren Zugang vorübergehend sperren lassen.



#### IV-Sicherheit an der WWU

Das IV-Sicherheitsteam bündelt die IT-Sicherheitskompetenzen von ZIV, IVVen und GB-IT und erarbeitet Sicherheits- und Betriebsregelungen. Es bietet im Internet eine umfassende, aber leicht anzuwendende Hilfestellung an, damit Sie Ihren Computer, Tablet-PC oder Ihr Smartphone selbst gegen die Gefahren im Alltag absichern können:

# www.wwu.de/iv-sicherheit

- Nützliche Software zu Ihrem Schutz finden Sie auf der Internetseite des IV-Sicherheitsteams.
- Verständliche Anleitungen & Videos erklären in wenigen Schritten die Installation und Einrichtung der Programme.
- > Ausführliche Informationen zur IV-Sicherheit helfen Ihnen dabei, weitere mögliche Gefahren für Ihren PC zu erkennen. Erfahren Sie, wie Sie sich schützen können und welche Hilfen das ZIV anbietet.



#### **Impressum**

Herausgeber: IV-Sicherheitsteam der WWU Röntgenstraße 7–13, 48149 Münster

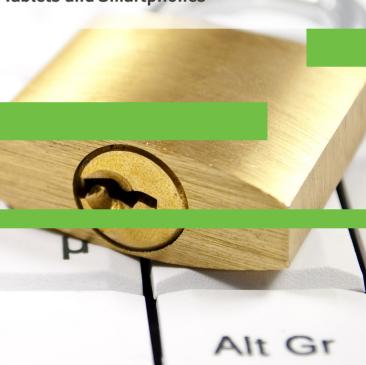
Fotos: P. Nunes/neirfy/M. Schuckart/B. Jackson

© Fotolia.com Stand: März 2017



# **IV-Sicherheit**

für Computer,
Tablets und Smartphones





### IV SICHERHEIT ERHEIT IV SICHERHEIT IV SICHERHEIT

#### Internet

#### Gefahren erkennen

- > Im Internet gibt es gefälschte Websites, böswillige Programme sowie Daten- und Identitätsdiebstahl.
- > Seien Sie aufmerksam und schützen Sie sich durch aktuelle Internetbrowser und Plugins.
- Beziehen Sie Downloads nur aus vertrauenswürdigen Quellen.

#### **Umgang mit E-Mails**

- Achten Sie bei Ihrem E-Mail-Programm auf eine verschlüsselte Kommunikation.
- Nutzen Sie die Möglichkeiten der WWU-Zertifizierungstelle (WWUCA) zur Verschlüsselung und digitalen Signierung von E-Mails.
- Reagieren Sie niemals auf E-Mails, in denen nach Bankdaten oder Passwörtern gefragt wird. Misstrauen Sie Links und öffnen Sie keine E-Mail-Anhänge, die ohne Anlass oder von unbekannten Absendern verschickt wurden.



# **Arbeitsplatz**

#### Nutzerkennung

- Arbeiten Sie im Alltag ohne Administratorrechte, um die Möglichkeiten von Schadsoftware zu begrenzen.
- > Sperren Sie den PC bei Arbeitspausen.

#### Betriebssystem- und Programmaktualisierungen

- > Installieren Sie regelmäßig Updates. Aktivieren Sie automatische Update-Funktionen und überprüfen Sie ggf. selbst, ob neue Updates für Ihre Programme vorhanden sind.
- > Arbeiten Sie nur mit Originalsoftware.

#### **Virenschutz**

- Installieren Sie ein Antivirenprogramm, um Ihren PC vor Schadsoftware (u. a. Viren und Trojaner) zu schützen. Das ZIV bietet eine solche Software zum kostenlosen Download an.
- > Führen Sie nach einem Virenbefall eine Neuinstallation des PCs durch.
- > Achten Sie auf eine aktive Firewall.

### **Datensicherung**

- Fertigen Sie regelmäßig Backups an, um Datenverluste zu vermeiden. Speichern Sie Sicherungskopien auf externen Datenträgern. Für universitätsbezogene Daten bieten ZIV und IVVen einen gesicherten persönlichen Speicherplatz an.
- Verschlüsseln Sie sensible Daten und mobile Datenträger, damit Unbefugte keinen Zugriff haben.

# Mobilgeräte & Apps

#### Allgemeine Empfehlungen

- > Sichern Sie Ihr Gerät mit einer PIN und aktivieren Sie die Geräte-Verschlüsselung.
- Verwenden Sie die aktuellste Version der Systemsoftware (Firmware). Installieren Sie nur Apps aus einem offiziellen App-Store.
- > Installieren Sie, falls möglich, einen Virenschutz.
- > Vermeiden Sie Jailbreaks/Rooting von Geräten.
- Achten Sie bei mobilen Internetverbindungen darauf, Ihre Daten verschlüsselt zu übertragen (z. B. über eine VPN-Verbindung).

#### Empfehlungen für Mitarbeiter

- Nutzen Sie das Exchange System für dienstliche E-Mails, Kontakte und Termine. Dadurch wird die automatische Umsetzung von Sicherheitsempfehlungen und eine Fernlöschung Ihres Geräts bei Verlust ermöglicht.
- Speichern Sie personenbezogene Daten nur auf Servern der Uni Münster.

