

Euren Computer und euer Smartphone nutzt ihr, um viele Dinge zu tun. Dabei sind nicht nur die offensichtlichen Dinge wichtig, die mit deinen Daten zu tun haben, sondern es sind auch vermeintlich alltägliche Suchanfragen, Browserbenutzungen und Dokumente sind mit wertvollen Daten verbunden. Also achtet im besten Fall bei allem was ihr tut darauf, dass ihr sicher unterwegs seid!

datenschutzfreundliche Browser:

- Firefox mit folgenden Addons:
 - uBlock Origin
 - HTTPS Everywhere
 - Duckduckgo privacy essentials
 - Privacy Badger
- **Tor-Browser**
- **Brave** (basiert auf Chromium Engine, hat ähnliche Features wie Firefox Addons integriert)

Suchmaschinen:

- DuckDuckGo

Mailclients:

- Thunderbird
- Claws
- K9 Mail auf Android (<https://k9mail.app/>)

Messenger:

- Signal
- Threema (kostenpflichtig)
- Element
- Jabber (Conversations Android App)

Cloud Storage (Dropbox/Google Drive Alternative)

- MyShare vom Rechenzentrum (<https://www.rz.uni-osnabrueck.de/Dienste/Myshare/index.htm>)
- Mega.nz (guter, verschlüsselter Online-Speicher)

Video(-Konferenz) Software:

- BigBlueButton (eigener Raum via: <https://webconf.uni-osnabrueck.de/>)
- Jitsi (<https://meet.osna.social> gehostet vom ChaosTreffOsnabrück)

Text Pads:

- CodiMD (<https://codimd.c3d2.de/>)
- Cryptpad (z.B. <https://cryptpad.ccc-mannheim.de/>)
- Etherpad (<https://pad.jmt.gr/>)

Tabellen Pads:

- EtherCalc (<https://calc.aachen.ccc.de/>)

Kommunikationsplattform (spez. Für Uni Osnabrück):

- StudIP: eigene Studiengruppe gründen und alle Funktionen von Studip für sich und andere nutzen.

Online-Security:

2-Faktoren-Authentifizierung bei allen Diensten benutzen, die euch wichtig sind. Die Uni-Mailadresse nicht einfach an eine andere Adresse weiterleiten lassen.

Passwortmanager (zur Sicherheit ab und zu Backups des Passwort Safes machen!):

- KeePass
- Bitwarden (<https://bitwarden.rz.uni-osnabrueck.de/#/>)

Verschlüsselung von Daten:

- VeraCrypt
- auf dem eigenen Betriebssystem die Verschlüsselung aktivieren
 - Windows: Bitlocker - nicht 100%ig sicher, aber besser als nichts
 - Apple: FileVault ist gut

Office Programme (Texte, Präsentationen, Tabellen):

- Libre Office

Sicheres Löschen von Dateien:

- Eraser

Video Player:

- VLC Media Player

Bildbearbeitungsprogramm:

- Gimp
- Metadaten löschen: Exif Tag Remover

PDF Viewer

- Okular (<https://www.heise.de/download/product/okular-96066>)

Backuplösung für Win10 (benötigt externe Festplatte):

1. Drücken Sie die Windows-Taste oder klicken Sie auf das Windows-Symbol in der Taskleiste (für gewöhnlich links unten).
2. Drücken Sie auf das Zahnrad-Symbol, das öffnet die Windows-Einstellungen.
3. Wählen Sie "Update und Sicherheit".
4. Klicken Sie im Menü links auf "Sicherheit".
5. Klicken Sie auf "Laufwerk hinzufügen" und wählen Sie ein Laufwerk. Das kann eine externe Festplatte, ein USB-Stick oder eine SD-Karte sein. Am besten ist es, wenn Sie ein leeres Laufwerk verwenden.
6. Unter "Weitere Optionen" können Sie bestimmen, wie oft Windows die Daten sichern soll. Auch lassen sich verschiedene Quellen wie Ordner oder der Desktop wählen

PC Betriebssystem:

- Ubuntu (Linux) in verschiedenen Designvarianten
- Fedora (Linux)

Smartphone AppStore:

- Fdroid (nicht alle Apps verfügbar, aber gute Alternativen)
- Aurora Store (greift anonym auf den Google Play Store zu)

Gute Linksammlung für Pads und andere Kollaborationsdienste:

<https://github.com/tosterkamp/random-redirect/>