

# Safe use of external storage media

## Risks inherent in using external storage media

- External storage media can be lost or stolen
- External storage media can malfunction
- Sensitive data can be viewed
- Malware can be installed on your computer

## Encrypt sensitive data

Every time you transport data on external storage data, you should protect them against unauthorised access.

- Encrypt individual files using encryption or document protection (e. g. available for Office files)
- Use encryption to protect your entire storage medium or sectors thereof

### External storage media

External storage media such as USB sticks, portable hard drives or CDs/DVDs are in everyday use with computers today. Their advantage is that they are mobile - they fit into any bag or pocket and are easy to take with you. However, this also harbours risks which must be considered.

## Securely delete sensitive data

When deleting sensitive data, you should use suitable tools to do so.

- Eraser (<http://eraser.heidi.ie>)
- Secure Eraser (<https://www.ascomp.de>)

## Deactivate autorun function

If you run Windows, you should deactivate the autorun function for all external storage media.

- Temporarily by holding down the shift key while connecting the device
- Permanently as described by Microsoft here (<http://support.microsoft.com/kb/967715/en>)

If you run Mac OS X, deactivate the CD/DVD autorun function.

- Permanently under Control Panel, under CDs & DVDs

Further information: [www.ebas.ch/externalstoragemedia](http://www.ebas.ch/externalstoragemedia)

«eBanking – but secure!» is offering helpful security hints for e-banking users

# eBanking but secure!

You will find further practical information on measures and approaches required to ensure that e-banking applications are used securely under [www.ebankingbutsecure.ch](http://www.ebankingbutsecure.ch). The use of this website is free.



Hochschule Luzern – Informatik  
Campus Zug-Rotkreuz, Suurstoffi 41b  
CH-6343 Rotkreuz