Secure deletion

Erasing data for good is more difficult than you would think, because there are various ways to delete and erase! The most secure solution - to physically destroy a data carrier - is not generally very practical. But there are alternatives.

You securely delete data by...

- using some specific tools to overwrite any shared data sections on your magnetic hard drive or data tapes (several times).
- using some specific tools to overwrite the whole storage area of electronic data carriers such as USB sticks, SD cards or SSD hard drives once.
- resetting a smartphone or tablet to its factory settings with device encryption activated.
- physically destroying optical data carriers such as CD-R/RW or DVD-R/RW.
- encrypting the whole storage area or sensitive content of all kinds of data carriers and destroying the key material.
- physically destroying data carriers.

With the right software, files deleted without taking special measures can often be restored. That's because data cannot actually be deleted, but merely overwritten with other data. The difficulty consists in trying to cover all the filing locations.

To definitively and irrevocably delete confidential data, you will need special tools and a process adapted to the type of data carrier involved.

Magnetic data carriers, such as hard drives or data tapes

Special software will overwrite the whole area of your hard drive or data tape where the data to be deleted were stored with (random) data patterns - usually several times. This process will erase data for good.

There are several products on the market, both available commercially or for free, for instance:

Windows

- **Eraser**: Download: eraser.heidi.ie (https://eraser.heidi.ie)
- **Secure Eraser**: You can find some good instructions (https://www.computerbild.de/artikel/cb-Downloads-Tuning-System-Secure-Eraser-Tipps-Anleitung-5697825.html) on the Computerbild magazine website. Download: www.secure-eraser.com (http://www.secure-eraser.com)

macOS

- **Permanent Eraser**: Download: www.edenwaith.com (http://www.edenwaith.com)

Electronic data carriers such as SSD hard drives, USB sticks or SD cards

For technical reasons, it is not possible to securely delete individual files on electronic data carriers such as USB sticks, SD cards or SSD hard drives.

One option is to completely overwrite the whole data carrier. However, all the contents are lost in the process. Alternatively, you can encrypt your data (see below).

Smartphones and tablets

To irretrievably erase data carriers installed in smartphones and tablets, you can reset your device to its factory settings with device encryption activated. But beware: All user data will be lost!

Android

1. Activate device encryption under **Settings/Security** and wait until this process has finished (which might take quite some time!)
2. Reset your device to its factory settings under **Settings/System/Reset options**

iOS

1. Recent iOS devices have encryption activated as standard, something which cannot be deactivated.
2. The Apple ID ensures that your device is still linked to you once you have deleted all data. If you would like to pass your device on, you will therefore have to delete the link to your Apple ID (before you delete your device contents) under **Settings/Sign out/Turn off**.
3. Reset your device under **Settings/General/Reset/Erase All Content and Settings**.

Another easy option to at least securely erase all of your stored photos and videos is to manually delete all content you no longer want, and then use the camera app to record a “blank” video, for instance while pointing the camera downwards onto a tabletop, until the phone memory is full. (Attention: This will also record sound, and some memory sectors, for instance those for messages, may not be deleted or overwritten this way).

Optical data carriers such as CD-R/RW or DVD-R/RW

As far as data deletion is concerned, too little attention is paid to optical data carriers such as CD-R/RW or DVD-R/RW. After use, they are often discarded as-are in the dustbin - and your sensitive data with them.

Due to technical problems (CD-R/DVD-R) or the small value of these data carriers (CD-RW/DVD-RW), it is often impossible to delete these data securely.

To physically destroy these data carriers is both a secure and practical method.

Physical destruction of data carriers

To physically destroy them is a secure method of erasing data carriers of all kinds. You can for instance drill a hole into a hard drive or smash a USB stick with a hammer to destroy its storage chip. A more professional and

guaranteed process complying with DIN standard 66399 is offered by commercial providers.

Physically destroying data carriers of course also destroys their value. For more expensive data carriers, such as larger SSD drives or devices with permanently installed data carriers such as smartphones or tablets, this is not generally a practical solution. In these cases, data encryption is a good alternative.

Protect by encrypting

The most secure and also most flexible alternative to erasing any type of data carrier is to encrypt data worth protecting and to thus render confidential contents unreadable for any third parties. In contrast to data deletion, this protection is effective over the whole data lifecycle and even subsequently. This is because once you delete the key material, all data are lost irrevocably.

To make sure that no unprotected contents are ever stored on any data carrier at any time, the whole data carrier should be encrypted as soon as you start using it. There is a variety of programmes available for this, too:

Windows

- **BitLocker** is a utility offered as part of all Windows Ultimate/Pro/Enterprise versions to encrypt whole data carriers.
- **EFS** is a NTFS file system function integrated into Windows as standard. This can be used to encrypt individual user-specific files or folders.
- **VeraCrypt** is free of charge, powerful and easy to operate. Download: www.veracrypt.fr (https://www.veracrypt.fr)

macOS

- **FileVault** is a function integrated into macOS as standard to encrypt both data and whole hard drives.
- **VeraCrypt** is free of charge, powerful and easy to operate. Download: www.veracrypt.fr (https://www.veracrypt.fr)

Data can be irrevocably destroyed by physically destroying data carriers. It is more practical though to use special software to “delete by overwriting”. Another alternative to this - effective over the whole lifecycle of data and beyond that, too - is to protect data by encrypting them.

Further information for those interested:

It is not sufficient to simply delete via the recycle bin or by formatting

With computers, files are generally moved to the recycle bin first. From there, you can recover your data if needs be, and they are seemingly deleted for good once you empty the bin. The latter however does not really "delete" the actual files, but only the directory link to the file. This renders the file "invisible" to users, and those areas of the hard drive containing the files to be deleted are earmarked for overwriting. These data keep existing until another file is written to the area marked for overwriting.

It is a similar case when formatting data carriers. When quick formatting, references to all files are removed from the directory. Yet, the file contents survive with this process - even if in the shape of orphaned files.

It is more effective to run a complete disk format. With today's operating systems, this will completely overwrite all storage spaces with zeros. It is therefore de facto impossible to recover any files by reasonable means.

You can therefore recover deleted data which have not been overwritten. This can be very helpful if you inadvertently delete a file you still need. However, for security reasons - for instance if you wish to delete a confidential file for good - this is not desirable.

To delete an individual file or a complete data carrier for good, you may need special software. The process depends on the type of the data carrier or the type of recording process used here:

Magnetic hard drives

On magnetic hard drives, the filing location of any file is precisely defined. Special software is therefore able to locate this specific hard disk area and to overwrite it - usually even several times, to be on the safe side. This process will erase data for good.

If you are thinking of disposing of or selling your computer, you should either remove its data carriers or at least make sure you delete all data on its hard drive. After all, you really don't want the buyer of your device to be able to retrieve your sensitive data. It is easiest to use a bootable CD with suitable tools which will overwrite the whole hard drive, for instance DBAN (https://www.dban.org) for Windows.

USB sticks and SD cards

For technical reasons, on so-called flash storage media such as USB sticks or SD memory cards, it is possible for the same contents to be stored in several filing locations. This results in the automatic creation of copies. When deleting by overwriting, only the copy last used will be deleted - the others remain.

You should therefore note that you can only ever securely delete data from a flash storage unit by irrevocably erasing the whole medium. There is basically no way you can securely delete individual files from USB sticks and SD cards.

SSD hard drives

Files on SSD hard drives now built into newer computers can therefore not reliably be deleted with the software mentioned above. This has technical reasons: To ensure the memory cells wear out evenly, the stored contents on this hard drive are automatically reorganised from time to time. This creates "lost" data copies which cannot be specifically overwritten. It is therefore not possible to reliably delete data by overwriting.

Some SSD hard drive manufacturers offer integrated functions which find and purportedly irrevocably delete such lost data on this type of data carrier. However, it is nigh on impossible to check that is function actually works and is really reliable.

In addition to the physical destruction of the data carrier, it is the same here with regard to files. You can only securely delete them if you delete the whole storage area of this data carrier.

Another secure alternative is to encrypt individual sensitive files or even the whole storage area of this data carrier to start with. Without key material, third parties are then unable to read confidential contents. This also has the advantage that your sensitive data are even protected if your device (for instance your laptop) is stolen or lost - no access without your key!

Optical storage media
With writable optical storage media, a laser engraves data into a reflective layer in a hole pattern. Depending on this layer, you can either repeat this process just the once (R) or several times (RW).

Due to the technical difficulties and the low value of these data carriers, it is the most practical solution to destroy these data carriers to delete your data.

Magnetic data tapes
Magnetic data tapes are often used to back up a whole data collection to retain them over extended periods of time. They therefore enable “looking into the past” - to even retrieve data long believed lost.

Magnetic data tapes back up contents to be stored in sequential data sets. These generally form an unchangeable unit provided with integrity protection. You cannot delete individual files from these. When deleting data, you have to destroy the whole data set instead.