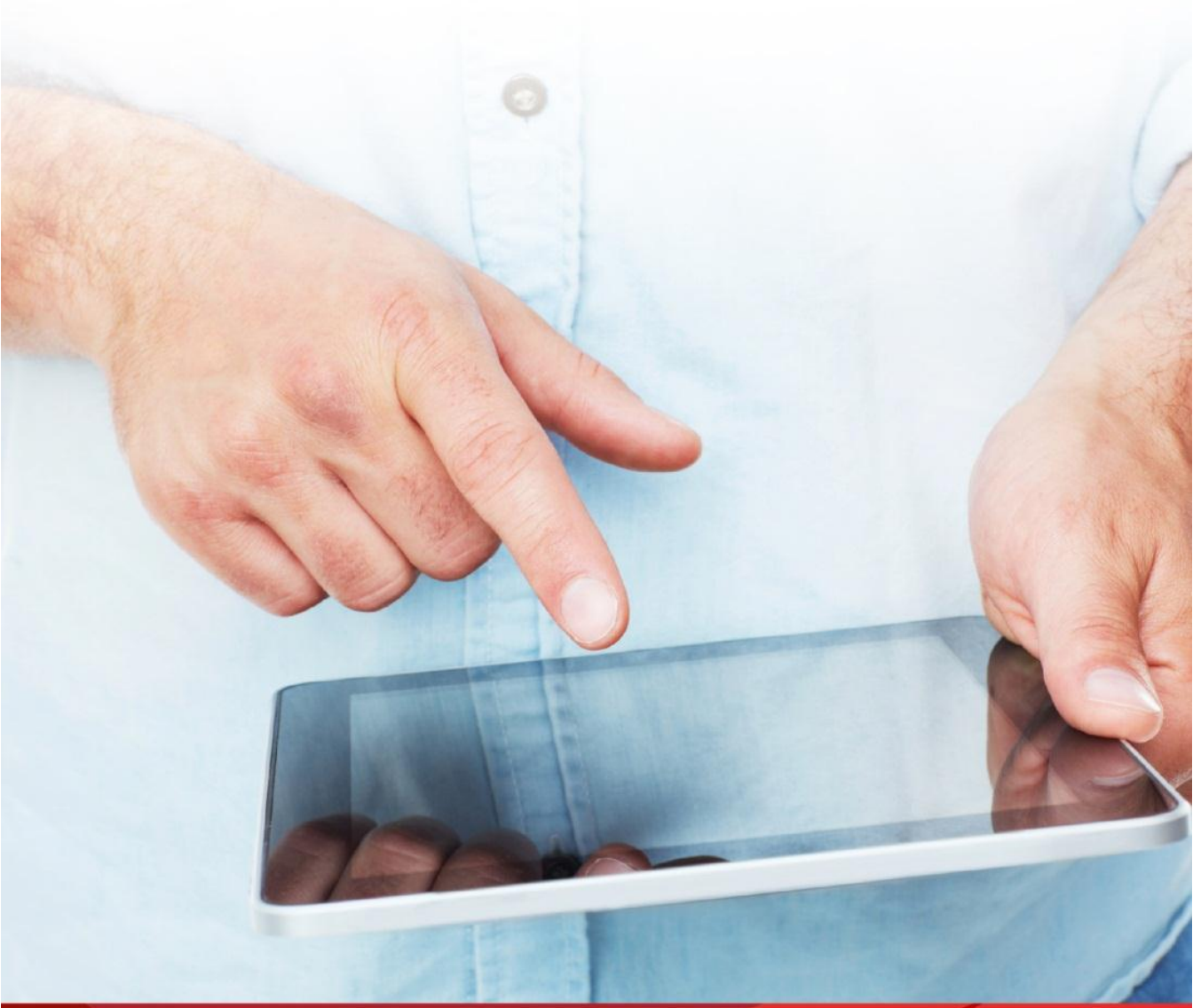
How to Erase Data Securely

A **TrendLabs** Digital Life E-guide



Getting a new computer or smartphone is always exciting but do you know what to do with your old one?

The truth is that it's not as simple as just giving them away or selling them.

You have to remember that these items contain personal files and information that you wouldn't want strangers or bad guys to see. Bad guys can recover the data stored in your old devices and use them for their own personal gain. Before you discard your old gadgets, make sure your data is completely removed with the following steps.

Locate Then Select

Before you proceed with deleting your files, make sure you know the location of all your important files. This ensures that there are no stray copies that could be viewed by strangers. For example, are all your work-related documents stored in a particular drive or are there copies in a flash drive somewhere? It's only logical to delete traces of those files in both formats.

Prioritize any data that contains personal or sensitive information. These can include any "official" documents, transaction receipts and other finance-related files, personal photos, software licenses, work-related documents and other documents with names, contact details, or passwords.

The trick here is to search for files that could compromise your safety or reputation. Once you're done deleting those, you can move on to deleting less important files (like that copy of your book report from ten years ago).

Choose Your Method

Your method of destruction would depend on what you plan to do with your old device. If you intend to sell or give it away, data wiping would be your best bet. If you just plan on disposing your device, you're better off destroying your drive or device.

People often assume that reformatting is just like data wiping and is enough to delete your files. But reformatting is not a permanent fix; there are specialized tools that allow you or someone else to recover data after reformatting. Data wiping, on the other hand, overwrites the data multiple times to make it non-retrievable. When it comes to data destruction, data wiping is the preferred method.

Clean Your Hard Drive

You have three options for deleting files on your hard drive.

Data Wiping – Data wiping overwrites hard drive sectors multiple times to erase your data from the hard drive. The recommended number of times required for overwriting data may vary but you can start with your selected program's default setting. Trend Micro Titanium offers *Secure Erase*, which allows you to completely delete data in your computer.

Degaussing – Degaussing involves having your hard drive demagnetized and rendered unusable. Degaussing machines are expensive but there are companies that offer this service to the public for a more affordable fee.

Destroying the hard drive – Destroying the hard drive is possibly the most effective way of ensuring your data remains deleted. While there are different ways to go about destroying your hard drive (smashing it, drilling holes, etc.), you should always remember to wear safety goggles and other protective gear.

Destroy CDs, DVDs, and Flash Drives

Destroying CDs and/or DVDs can be done with the proper tools. You can use a pair of specialized scissors or a shredder that also handles CDs. You can also “scratch” the data off by removing the upper metallic layer with rough sandpaper but this takes a long time and can be inefficient.

Whatever the method, it’s always important to use protective gear. Safety goggles and gloves can protect you from sharp bits and pieces. Destroying your CDs and DVDs inside a large bag can prevent debris from flying around.

Just like your hard drive, you can wipe your flash drive to delete the data. However, destroying flash drives is still the most secure way of permanently deleting all traces of your files.

Secure Cloud Accounts

Deleting data stored in cloud services is trickier because you can't be sure that your data has been completely deleted (compared to smashing a hard drive).

With that in mind, it's best to limit the amount of sensitive information you store or share online. You can also read privacy policies or contact the cloud services directly to find out their policies on data deletion.

It's also important to protect your data while it's stored in the cloud. Protect your account with strong passphrases. You can even use a password manager to create one for you. Avoid sharing access to your accounts.

If possible, encrypt all your data. Encryption uses a mathematical formula to encode all your data to make sure that you're the only one who can read or access it, and acts as a last line of defense in case someone manages to access your accounts. Encryption software is available but you can also choose cloud services with built-in encryption.

Deleting Mobile Data

People often forget that mobile devices can contain sensitive information. Luckily, there are different tools and apps available that can erase your files for you.

It's also recommended to do a factory data reset after deleting your files to make sure they remain deleted. Just make sure to double-check even after a factory reset. There have been reports that some data remains on the device after undergoing the reset process.

Since a lot of users use SD cards for their phone, it's also recommended that the SD card be wiped clean or destroyed.

Dispose Old Devices Properly

After wiping all the data, you can also throw away old devices to make sure no one else gets to them. But don't assume electronic devices are "regular" trash. You cannot just chuck them into your trash cans and call it a day.

You should always go to an electronics recycling or disposal center to make sure your devices are properly destroyed without harming the environment. Some disposal centers are even held accountable for devices they destroy, which reduces the chance of data leaks.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

©2013 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

TREND MICRO™

Enjoy your digital life safely

Created by:
TrendLabs, The Global Technical Support & R&D Center of TREND MICRO