

What is the Schneier (Data Sanitization) method?

The Schneier method is a software-based Data Sanitization method used in some file shredder and data shredder programs to overwrite existing information on hard drives or other storage devices.

The Schneier method is a software-based Data Sanitization method used in some file shredder and data shredder programs to overwrite existing information on hard drives or other storage devices.

Deleting your hard drive by Schneier method will prevent all software-based file recovery methods from finding information on the drive and also prevent most hardware-based recovery methods from extracting information.

In a nutshell, the Schneier method overwrites data on a storage device with a number, followed by a zero and finally with a few random characters. More details on this method will be found below, along with a few examples of programs including the Schneier method as an option when deleting data.

What does the Schneier method do?

All Data Sanitization methods work in the same way, but they are not always done the same way. For example, the Write Zero method just overwrites data with zeros. Other methods, like Random Data, only use random characters. HMG IS5 is very similar in that it overwrites the number 0, then the number 1 and then the random character, but only one time overwrites the random character.

However, with the Schneier method, there is a combination of multiple rewrites of random characters as well as zeroes and zeroes. Here is how this method is usually done:

1. 1st time: Override number 1
2. 2nd: Overwriting the number 0
3. 3rd: Override a series of random characters
4. 4th: Override a series of random characters
5. 5th: Override a series of random characters
6. 6th: Override a series of random characters
7. 7th: Override a series of random characters



Schneier method

Tip : Some programs may use the Schneier method with minor variations. For example, some applications may support verification after the first or last override. What they do is confirm that the character is actually written to the drive. If not, the software can tell you or just automatically restart and run the overwrites.

There are several programs that allow you to customize the rewrites, such as adding 0 after the second. However, if you make too many changes to this method, Schneier no longer holds true. the nature too. For example, if you remove the first 2 records and then add a few more random characters, you will switch to the Gutmann method.

Schneier support programs

A number of different programs allow you to use the Schneier method to erase data. Some examples are Eraser, Securely File Shredder, CBL Data Shredder, CyberShredder, Delete Files Permanently, and Free EASIS Data Eraser.

However, as mentioned above, some file shredder and data shredder programs allow you to customize what happens during the overwriting process. This means that even if they do not already have this method, you can "build" the Schneier method in programs, using the above structure.

Most data destruction programs support a variety of Data Sanitization methods in addition to the Schneier method. If you want, you can choose another method of deleting data after opening the program.

You finished reading the article "**What is the Schneier (Data Sanitization) method?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.