

# The way to stop people from copying files to a folder is to use NTFS security, not to block drag/drop

 [devblogs.microsoft.com/oldnewthing/20090826-00](http://devblogs.microsoft.com/oldnewthing/20090826-00)

August 26, 2009



Raymond Chen

A customer wanted to prevent users from copying files to certain locations, and they did it by hooking functions like `SHFileOperation` and failing the operation if the parameters were not to its liking. The customer found that the hooks stopped working in Windows Vista because Explorer in Windows Vista uses the new `IFileOperation` COM interface instead of using the old `SHFileOperation` function. The customer wanted assistance in getting their hook working again so they could prevent users from copying files to directories they wanted to block. Well, first of all, arbitrary function hooking is not supported by any version of Windows, so the customer was already in unsupported territory right off the bat. (There are some components which have an infrastructure for hooks, such as file system filter drivers or Winsock Layered Service Providers.) Second, attempting to hook `SHFileOperation` to prevent the user from copying files into specific directories is looking at the problem at the wrong level, similar to the people who want to block drag/drop when what they really want to block is accidental drag/drop. If you block copying files via drag/drop in Explorer, that won't stop the user from copying files by other means, or by doing the "poor man's copy" by opening the document from the source location and doing a *Save As* to create a duplicate in the destination. If you want to prevent the user from copying files to a directory, use the NTFS security model. Withhold *Create files* permission in the folder, and users will be blocked from copying files into the directory in Explorer, Notepad, or any other program.

**Related:** Shell policy is not the same as security.

Raymond Chen

**Follow**

