

## Is a File Really Deleted When You Hit “Delete”?

Have you ever wondered what happens when you delete a file from your computer? You hit the delete button, send it to the Recycle Bin, and then empty the bin, thinking it's gone forever. But is it really? Let's find out what's happening behind the scenes.

### Where Does a Deleted File Go?

Think of your computer's file system like a book. When you delete a file, it's like removing the title from the book's index. The reference to the file is gone, but the actual content, or the page, is still there until something new is written over it.

So, when you delete a file, your operating system marks the space as available for new data but doesn't immediately remove the file itself. This is why you can often recover deleted files using special software: the data hasn't actually gone anywhere.

### Accidentally Deleted a File? No Problem!

We've all been there, accidentally deleting an important file and then panicking. The good news is that as long as that space on your hard drive hasn't

been overwritten by new data, you can usually get the file back. There are various data recovery tools available that can scan your hard drive and restore those seemingly lost files.

Think of it like this: you've removed the title of a chapter from the book's index, but the chapter itself is still there. With the right tools, you can find and restore that chapter back to the index.

### Deleted for Good? Maybe Not

On the flip side, what if you intentionally delete a file because you want it gone forever? Maybe you're selling your computer and want to ensure all your personal data is wiped clean. Simply emptying the Recycle Bin isn't enough.

Just like in our book analogy, the content is still there, even though the title is gone from the index. Until those "pages" are overwritten, the data can be recovered. This is where things get a bit more technical.

### Making Sure It's Really Gone

To permanently delete files, you need to go beyond just hitting delete. Here

are a few methods to ensure your data is truly gone.

**Overwrite the Data.** Use special software to overwrite the deleted files with random data. This is like scribbling all over the pages in our book until the original content is illegible.

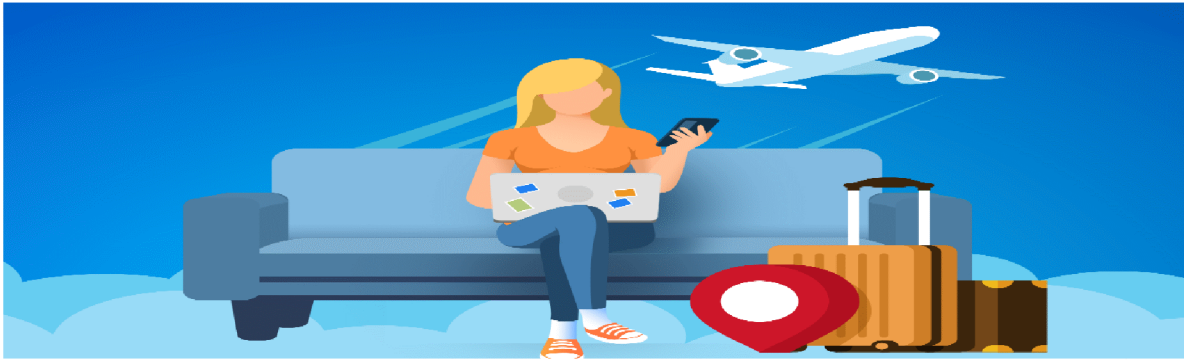
**Encrypt Your Drive.** By encrypting your drive, even if someone tries to recover the deleted files, they will get only a bunch of unreadable encrypted data.

**Destroy the Drive.** For the ultimate data destruction, physically destroy the storage device.

### Final Thoughts

Deleting a file isn't as straightforward as it seems. Whether you're looking to recover an accidentally deleted document or make sure your personal data is gone for good, it's important to understand how file deletion works. Always use reliable tools to manage your data securely and effectively.

**If you ever need help with data recovery or secure deletion, feel free to reach out to us. We're here to help keep your data safe and secure, no matter what your needs are.**



## Travel Smart: Data Security Tips

Planning a trip is always exciting, but keeping your personal information safe while on the go is extremely important. Here are some simple and practical steps you can take to protect your digital privacy when you're travelling.

### Encrypt Your Devices

Let's start with encryption. This is a fancy way of saying that your data is locked up tight and can't be accessed without your password. Newer Apple and Android devices are already encrypted if you have a password or PIN set up. If you don't have one, now's a great time to add one. For MacOS and Windows laptops, you'll need to turn on encryption manually. The big benefit is that if your device gets lost, no one can access your data without your password.

### Turn on the "Find My Device" Services

Next, make sure you've enabled "Find My Device" services on your gadgets. This allows you to track your device's location if it goes missing. For your other belongings, consider using Apple AirTags or Tile trackers. These little devices can help you keep tabs on your stuff, giving you one less thing to worry about.

### Don't Leave Devices Unattended

It might seem obvious, but never leave your devices unattended. Thieves often go for easy targets, and a device that's left out in the open can be a prime opportunity. This is especially risky if your device is still logged in and not on the lock screen. Keep your devices close and secure.

### Keep Your Devices Updated

Make sure all your devices and software are up to date. Updates often include important security fixes that protect against new threats. Plus, it's easier to download updates at home where you have faster and cheaper internet. This way, you avoid the hassle of dealing with slow or expensive Wi-Fi while you're travelling.

### Avoid Public Wi-Fi

Public Wi-Fi might seem convenient, but it's also a hotspot for hackers. Sometimes, malicious hotspots are set up with names such as "Cafe Free Wi-Fi" to trick you into connecting. Once you're on, they can intercept your data or even serve fake login pages to steal your information. It's best to avoid public Wi-Fi whenever possible. If you need internet access, use your phone's data plan or a personal hotspot instead.

### Use a VPN

If you absolutely have to use public or hotel Wi-Fi, a Virtual Private Network (VPN) is your best friend. A VPN encrypts your data before it leaves your device, sending it through a secure server before it reaches its destination. Think of it like sending a locked box through the mail: it prevents anyone in between from seeing what's inside. This added layer of security can help keep your information safe from prying eyes.

### Don't Use Public Devices to Log into Your Accounts

Logging into your accounts on public computers is a big risk. These devices can have keyloggers or other malware that capture your login details. Plus, there's always the chance you might forget to log out, exposing your accounts to the next user. Stick to your own devices whenever possible.

### Backup Your Devices at Home

Before you head out on your trip, make sure to back up your devices. This way, if your device is lost or stolen, you still have access to all your data. On some devices, you can create a copy of the entire operating system and its data. If you get a new device, you can restore everything and have it look just like your old one.

## Quick Recap For Travelling Smart:

1. **Encrypt your devices.** Set up a password or PIN and enable encryption on your laptop.
2. **Turn on "Find My Device" services.** Use GPS tracking for your devices and consider AirTags or Tile for other belongings.
3. **Don't leave devices unattended:** Keep your devices secure and close by.
4. **Keep your devices updated:** Download updates at home to avoid slow and expensive Wi-Fi on the go.
5. **Avoid public Wi-Fi:** Use your phone's data plan or personal hotspot to avoid potential hackers.
6. **Don't use public devices to log in to your accounts:** Stick to your own devices to avoid malware and keyloggers.
7. **Use a VPN:** Encrypt your data when using public or hotel Wi-Fi.
8. **Backup your devices at home:** Ensure you have access to your data in case your device is lost or stolen.

Travelling should be fun and stress-free. Following these simple steps allows you to enjoy your trip without worrying about your digital privacy.

**If you need help preparing your devices for your big trip, give us call at 940-282-0290.**