Deleting Sensitive Information? Don't Rely on Your Recycle Bin

Presented by C.J. Ferrari and Mark Miller

Computer forensic experts are a lot like paleontologists—the scientists who study the life of past geological periods. Paleontologists have never unearthed a full dinosaur skeleton. But, by examining just a small sample of scattered bones, they've been able to figure out the skeletal structure of hundreds of dinosaur species.

Likewise, when we delete our computer data by conventional means (i.e., moving a file to the Recycle Bin and emptying that bin), we leave "fossils" or remnants behind. And the paleontologists of the digital world—namely, computer forensics experts and savvy cybercriminals—can use those remnants to put together a full picture of the data we'd tried to delete.

So what can you do when you want to remove information from your hard drive? Let's take a look at what really happens when you delete files, as well as how to erase data so that no one can reconstruct its "skeleton."

Why emptying the Recycle Bin just won't cut it

To best understand how your Recycle Bin treats your data, think about what you do when you repaint a wall in your house. Do you first take the old paint off? Of course not. You paint over the old coat, either with a primer or the new color.

Similarly, when you empty your Recycle Bin, you aren't removing that data. You're only marking it for overwriting. If you can think of your unwanted data as that old coat of paint, all you're doing is hanging a sign on the wall that says, "TO BE REPAINTED." The data is only gone when you add new data to that location—overwriting it.

Here's the problem: you can never be sure where the data that needs to be overwritten is located, so you never know which remnants are still around and which aren't. Someone well-versed in data recovery can take those remnants and figure out the rest. The Recycle Bin just doesn't do the trick.

Don't rely on encryption either

Put simply, encryption is a way of scrambling data so that unauthorized users can't read it. It's the most secure means of keeping your data private when it's *actively in use*.

But if you were to toss your encrypted drive in the trash, you never know if it will fall into the wrong hands. At that point, it isn't impossible to recover the decryption key and access the data—especially for those who make a living off of harvesting and exploiting sensitive information. In the trash, your encrypted hard drive is at much greater risk than when it was sitting in your locked home or office.

Recommended solutions

Your Recycle Bin will suffice for getting rid of unimportant files, but for a hard drive full of sensitive information, you'll want to try one of the following methods:

1. **Physical destruction.** Shredding. Burning. Hammering. Physical destruction is the easiest, cheapest way to get rid of data. But its effectiveness is hard to quantify. What if an attacker puts the hard drive back together—and it *works*? Instead of placing the hard drive under your tire to crush it, consider having it professionally destroyed by an electronics recycling service. (You can find these services online or at your local tech or electronics store.)
2. **Full-disk overwriting software.** As mentioned, your data is still alive on your computer as long as it hasn't been overwritten by new data. Certain programs can overwrite an entire drive with multiple layers of random data (like multiple coats of paint), making it significantly more difficult to uncover the original data.
3. **Degaussing.** A degausser is a device that erases all magnetic data on a hard disk and renders the disk unusable. Today, this is one of the most effective data-destruction methods, but it's typically too expensive for personal use. As with physical destruction, you may want to reach out to a professional electronics recycling service.

Keeping the fossils buried

In a world where technology is becoming exponentially more convenient, it's still surprisingly difficult to completely delete files. We hope you find these tips useful in keeping your data dinosaurs safely buried.

###

CJ Ferrari and Mark Miller are financial advisor located at Miller Ferrari Wealth Management, 400 SW Bluff Dr., Suite 107, Bend, OR 97702. They offer securities and advisory services as Investment Adviser Representatives of Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. They can be reached at 541-639-8055 or cj@millerferrari.com or mark@millerferrari.com.

Authored by the Information Security team at Commonwealth Financial Network.