

<http://www.venturacountystar.com/news/2007/jul/31/usb-flash-drives-are-easy-to-use-8212-and-lose/>



USB flash drives are easy to use — and lose

By Allison Bruce ([Contact](#))
Tuesday, July 31, 2007

USB flash drives are everywhere.

Tucked into pockets, purses or hung around necks as a sort of honorary badge of geekdom, there's no escaping the ubiquitous storage devices. Call them what you like: thumb drives, key drives, flash drives, stick drives.

They provide flexibility and durability — not to mention a lot more space — than the once-popular floppy or even writeable CD. They make copying and transferring files a lot easier. And they're also easy to lose.

Hence the double-edged sword of the flash drive. Much easier to store and back up files on, they also make it much easier to sneak out corporate secrets or accidentally drop sensitive files on a busy street.

Some companies have banned employees from using them.

Others take a more practical approach.

At HRL Laboratories in Malibu, new ideas and proprietary information are commonplace. The company is a research and development laboratory owned by Boeing and General Motors. In addition to the work it does for those two companies, it does contract research and development work for the U.S. government and other companies.

HRL won't allow cell phones inside that can take photos — to keep information more secure.

Flash drives fall under the company's existing security policies, which include requiring anyone who makes a copy of a file to remove that copy, said David Weeks, media services department manager.

At telecommunications company Verizon, employees are discouraged from using flash drives, but if they do, they have to use very strong encryption, spokesman Jon Davies said.

The company has a section in its corporate policy code of conduct about using storage media.

It's "pretty strict because of the sensitivity of customer information and other sensitive data that employees have access to," he said.

Whenever possible, employees are encouraged to use something besides removable storage, he said.

"The likelihood of getting the information in the wrong hands increases when it becomes removable," Davies said. "That's always a concern."

At California Lutheran University, most students have a flash drive these days. The switch has been a positive for the Thousand Oaks campus, said Zareh Marselian, director of information technology.

This fall, the university is considering giving each incoming freshman a flash drive with their important handouts and orientation documents already saved.

The drives hold more, making them more useful to students, and they tend to be less vulnerable to viruses. Marselian said viruses overall tend to be less of an issue than they were in the late 1990s and early 2000s. Part of that is because there is a lot more awareness, and people keep their antivirus software up to date.

"We worry a lot more about spam than we do viruses these days," he said.

For those who do have important documents on their drives, such as the faculty and staff, Marselian said he recommends getting a drive that has a password-protected area to keep those documents safe even if the drive is lost.

And losing the drive is a common complaint.

"They're a lot easier to lose because they're smaller," he said. "You need to have a backup that does not go away."

The devices are getting smaller even as the amount they can hold grows larger.

Back in 2004, flash drives averaged about a third of a gigabyte in capacity, according to Semico Research Corp. That average is now at more than two gigabytes and is expected to top 13 gigabytes by 2010. As storage space goes up, cost has come down, making them even more popular to use.

"Over time, we're going to see these flash things increase in use, no doubt about it," said John Emerson, information technology manager for the city of Ventura.

Technology changes so quickly that policies demand an annual review to keep up to date, he said. City employees tend to port around Word or Excel files on their USB drives that they can work on at home.

The city is working on a security policy that would make sure that employees stay up to date on their virus protection on their home computers. The city is also looking at an in-network monitor to keep its network safe from viruses that may come into the office attached to a document that an employee was working on at home.

Similar to a firewall, which keeps viruses out of the network, an in-network monitor recognizes and isolates viruses already in the network.

"It's kind of neat we've got such dedicated people that want to work at home. We don't want to discourage that," Emerson said.