

Thumbs can be a bad thing!

Most of you own a cell phone and chances are you have lost or misplaced your charger causing you to look all through the office, car and home, only to be forced to purchase a replacement. I, too, have fallen victim to this syndrome.

Last week upon returning to the same hotel I had stayed at the previous week, I asked at the front desk if they had found a cell phone charger in my room. The desk clerk looked at me and then disappeared. A few moments later he emerged with a laundry basket full of cell phone chargers! I was amazed at the number and the variety in the basket. Here's a tip: before you purchase a replacement for a lost phone charger, drop by the front desk of the next hotel you stay at and ask them if they have any.

Moving on, I decided to conduct an informal survey on the way home from this business trip. Of course we know the answer to the question, "What electronic accessories are most often left behind at hotels?", but what about airport security and air travel?

Visiting with TSA, I found that the most common item left at airport security screening areas are cell phones. Two officers in the group quickly added, however, that the number of laptops and net books left behind is growing. The other security officers in the group nodded their heads in agreement.

On board my flights, I asked the crew the same question. Most flight attendants responded that they find thumb drives most often, in the seats, on the floor or in the seat back pockets. Any small place is a perfect spot to leave a thumb drive. During peak business travel periods they find a lot. (If you don't use these devices, a thumb drive, or jump, or USB, or flash drive is a portable storage device that can be purchased at any office supply store. They often are given away at conventions and workshops, and come in a wide range of storage sizes (some capable of storing many megabytes of data).

It is one thing to lose a charger. Forgetting a laptop can be another issue. At least you stand a good chance of having the laptop returned if you lose it at a security check point as opposed to a cab. The real alarming statistic of my unofficial survey is the thumb-drive revelation!

Thumb drives are a terrific tool; they're convenient, can store a tremendous amount of information, are inexpensive, portable, and compatible with any computer that has a USB port. These benefits are what makes them so dangerous.

Putting things into perspective, as inexpensive as a thumb drive can be, to lose one can cost you and your organization a lot more than money if the drive you just lost had sensitive customer information on it. The severity of the situation may exponentially increase if it falls into the wrong hands.

All financial institutions should take an immediate look at the policies and procedures in effect pertaining to the use of thumb drives. Our recommendation is that the use of thumb drives should be strictly controlled and not approved for casual use. The Information Security Policy and End User Policies of your organization should be strict and clear regarding the type of information that is allowed on a thumb drive. Further, regardless of the type of information, all thumb drives should be password protected and encrypted—at a minimum. Thumb drives should not be

purchased by employees, but issued (serial number and model) by the financial institution and periodically checked by the information technology department.

Finally, if one must use a thumb drive, use the drive responsibly. Protect the data by using hardened passwords and data encryption. Additional protection in exchange for some slight inconvenience is always a good policy.

The Wombat!

About the Author

Dan Fisher is president and CEO of The Copper River Group, a consulting firm headquartered in Fargo, N. D., that focuses on technology and payment systems research and consulting for community financial institutions. For nearly 30 years, Fisher has worked in the financial industry using technology to improve the bottom line. He was CIO of Community First Bankshares (now part of BancWest), has served as a director of the Federal Reserve Board of Minneapolis, the chairman of the American Bankers Association Payment Systems Committee, and was a member of the Independent Community Bankers of America Payments Committee. Fisher has written numerous articles on banking technology and the payments system. He has authored or co-authored six books and recently published a book titled, "Capturing Your Customer! The New Technology of Remote Deposit." You can contact Fisher at dan@copperwombat.com.

P.S. To understand Dan's nickname, check out "About the Wombat" on his website, www.copperwombat.com