

The smart phone has gone viral, and so have the risks

Can the smart phone be the key to your dreams? According to Assa Abloy it can.

* * *

The manufacturer of door locking devices, has developed an integrated system which enables hotel guests to make reservations online, check in, and receive an electronic key to their room and ultimately check out using a smart phone app in combination with a near field communications (NFC) chip embedded in the phone.

The NFC device is the same system that contactless cards and key fobs use today. It is a small authenticated transponder that transmits a code with your information to the receiver when the phone (chip) is passed over a contactless pad such as a point of sale terminal. Pass n Pay… It’s fast and simple. NO cash and NO math at the point of sale.

Combine the versatility of the smart phone with the NFC chip and the phone has become what the Wombat would define as a “VSCD” or a Very Small Computing Device. It is no longer a cell phone or a smart phone because it goes beyond just talking or touchpad communicating. The versatility of the device is reaching into every facet of our daily lives with new applications being devised faster that we can read about them, like the one just described.

The pairing adds a new dimension to the contactless world, but is the mainstream user fully aware of the risks? The risk receiving the most press, of course, is texting while driving. And despite the warnings, more drivers than ever seem to be reading and texting while driving.

Clearly the cell phone has become more important than a wallet or purse. Now, thanks to Assa Abloy, you can use it as a key. Next you will be able to start your car from the airplane as you are pulling up to the terminal, or open the garage door using a voice command. With all of this versatility comes information about the user that, if not properly protected, can expose the individual to unknown and unprecedented risk.

Yes, the smart phone has gone viral not just from the standpoint of explosive growth in users and applications, but also in consequences not fully realized yet. Smart phones are the new medium to the banking public, but the potential risks should be thoroughly considered prior to implementation because you know the question you will be asked by your customer when a serious compromise occurs: “Why didn’t you tell me that this small device was so dangerous?”

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