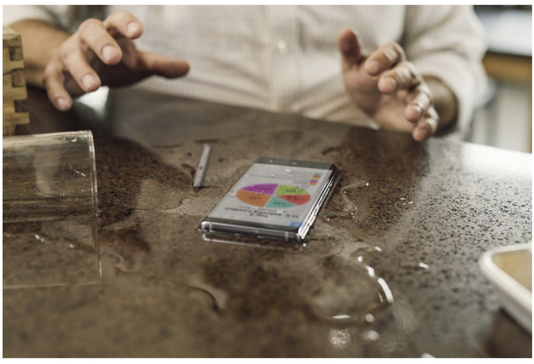
BACKCHANNEL 11.14.17 01:24 PM

PUTTING ALL YOUR DATA IN ONE SMARTPHONE BASKET



CARMEN CHAN

This content was produced by WMG Brand Lab in partnership with Samsung Knox

If your smartphone isn't within arm's length right now, feel free to start to panic. We'll wait while you tear apart the couch, office, car, or your bag to find it.

Everyone has had that moment of dread when we reach for our constant gadget companion and it's not there. Usually we find it, wedged under a driver's seat, or abandoned in some restaurant or yoga studio. Other times our smartphones are just gone, and it's time to deploy the kill switch.

That reaction, emotion – however you want to describe it – is proof of our reliance on these powerful and powerfully convenient devices. Losing a laptop is no treat either, of course, but most people don't have them with them all the time. Your phone is easier to lose. And as smartphones keep leveling up in performance and capabilities, most of us are fine leaving the bigger machines behind more of the time, especially when it comes to work.

For the people that run your corporate IT world, smartphones are also a constant companion, though persistent headache, might be a more apt description.

Kevin Baradet is the Chief Technology Officer and Facilities Director at Cornell University's SC Johnson College of Business. That means he is responsible for managing the technology infrastructure and needs for faculty, staff, and graduate-level students (think a lot of MBA candidates). At the end of every semester, Baradet is presented with a box full of lost phones from students, faculty and staff, no owner in site. Typically, none is ever found.

"I don't know if they have great insurance plans," Baradet says, "but how could they not miss them?" Especially if they knew what can be divined from a single smartphone.

Former federal agent turned private investigator Thomas Martin, president of Martin Investigative Services out of Newport Beach, CA, describes your mobile phone number as the "new social security number." With just a smartphone number, Martin says, investigators and information brokers have a window into "private information that is stored by almost all business corporations, financial institutions and – thanks to us – social media networks...It is like looking into your living room of life."

And that is with just a number. Now what about having the phone itself?

"Depending what you have on the smartphone you are putting your reputation at risk, you may have a contractual obligation to a third-party for consulting or research you are doing, and if you expose that information, well, what is the cost there?" Baradet says.

The question of who bears that cost at Baradet's school is straightforward – it's the owner of the phone. Cornell doesn't offer job related allowances for smartphones, but at the same time it's a work tool that most people need to do their jobs. That puts Baradet, and many others running IT shops in a delicate spot. They can recommend approaches, but without helping to foot the bill for a phone they don't have a lot of leverage with people. What Baradet does is resort to what he calls a "light touch" approach, providing best practices with an understanding that it is the user who is ultimately responsible if a phone is lost and breached.

"If you don't want to be responsible for the information you access on a smartphone, then don't access it," he advises his people. "And if you want, for example, a Microsoft client on your phone so you can access Office, well then know if you lose your phone we may send a silver bullet down the wire and kill it – photos and all – so are they backed up?"

Baradet offers his best advice: use a PIN, the longer the better; turn on your consecutive failure feature; encrypt the data on any removeable storage; backup sensitive or important data; and have some way to locate your phone if it is lost.

For the truly lazy among us, biometric security is getting better and better. Gone are the days when you had to sweep a finger across the fingerprint reader over and over only to eventually enter a PIN. And the really attractive thing for users about biometric verification? It makes security something we have to think less about. You just want to make it hard when that phone goes missing, Baradet says.

"You want to put some speed bumps in the way of anyone who may get their hands on your phone," he says. "Think about what is on your phone, and if I were to walk up to you and take it, what would happen? What would be the consequences?"

Of course, most people ignore his advice, Baradet says, until someone loses a phone and important data along with it. "I would say for the vast mean population of people – plus or minus two Sigmas – they will only adopt whatever doesn't get in their way. They don't even think about these sorts of risks."

Until something happens to themselves or a colleague. Then Baradet gets a flood of calls about what to do, and how to take pre-emptive measures. At least while the details of the hassle, or cost of losing data is still making the rounds.

"Look, Mark Twain had it right, now it just applies to smartphones." Baradet says. "If you put all your eggs in one basket, you better watch the basket."

#SMARTPHONE #KEVIN BARADET #PHONE #THOMAS MARTIN #SAMSUNG KNOX