

Digital Collateral Damages

One recent day a discussion that began with remote car starters, and quickly moved to smart phone insecurities and theft unearthed a phrase heard frequently in response to security suggestions. "I don't care if they steal my phone and read my email, I have nothing to hide." Not caring is one thing, but thinking there is nothing worth stealing inside that phone is another. The typical smart phone is not pin protected. The unlock instructions are clear and concise, and the actual lock is meant to prevent accidental pocket dials versus ensuring privacy remains. This means that all the SMS entries and personal photos are available for viewing. Calendar entries stating when others or even the phone owner are on vacation may be present. Contact information many times including addresses is trivial to extract as well. If the theft of the phone is an indication, a thief having an address and a known empty house should be a big concern. This brings up an interesting point about personal disclosure responsibility. An ethical discussion for later, but what about that email? As this particular conversation unfolded, the recent Twitter hack was mentioned. How the password reset function was exploited through re-registering an old and unused address, and having the freshly reset password sent to this. The gears were starting to turn when the question of what email account is registered with your bank was posed. Yes, that is right, the security of your banking relies upon the "slide to open" bar on that iPhone. Seeing the collateral impact of event is not always clear. The ripple effect is always in play which is why exercising even moderate best practices throughout the day can make a significant difference when it counts. Security is always as good as the weakest link. As the digital existence expands and blends more time needs to be spent on awareness. Far too many don't understand the risks they face, and until they do, they will never properly protect themselves.