Don’t Use SMS for Money. Or Secrets. Really.

Usability vs. truly effective security — can you have both?

The principle transcends technology: why rob the bank, with all those guards, when you can wait outside and rob customers? This January, hackers didn’t bother with the bank, they went after the online customers, quite successfully. To keep mobile banking transactions secure, the bank used two-factor authentication, sending customers text messages — over their telecom network — with a unique code. Users entered the code on their devices. It’s a simple technique, easy to use, but without additional encryption, quite vulnerable.*

Most telecom networks worldwide use Signaling System 7 (SS7) protocols for a variety of signaling tasks, it’s been around since 1975. By design, it enables fast, easy communications over phone networks. But the same design features also make it vulnerable to hackers. It’s just not that hard (relatively speaking) to track a phone's location, read or redirect messages, and even listen to calls. Most experts agree that fixing SS7 isn’t the answer — adding layers of firewalls and exotic filters would be like putting a Formula 1 engine on a bicycle.

Encryption, end-to-end, works much better. Indeed, if online banking uses non-SMS texting, such as iMessage, it’s much less of a problem. But that brings up other issues. Not all device manufacturers want to add a fingerprint reader or iris scanner, features that are easy for consumers and that improve security considerably. And expecting users to remember varied, complex passwords for all their apps — Keychain notwithstanding — isn’t realistic.

Usability vs. truly effective security — can you have both? Yes, and as usual, brains win over brawn. The math behind multi-party computation is enabling software-only authentication and key-management solutions that are thoroughly disrupting the security industry. Now, a high-volume, low-cost, connected consumer device — the archetypal product of the Internet of Things — can feature superior, hardware-level security with a virtual solution. COMPANY Security is enabling easy-to-use, real security for the IoT.

But meanwhile, don’t use SMS for money or secrets. Really.

Share this with your friends, so they’ll believe you when you tell them not to use SMS texts with mobile banking! Names have been omitted to protect the innocent.

** NIST deprecated the use of SMS-based out-of-band (SS7) authentication in its DRAFT NIST Special Publication 800-63B, Digital Authentication Guideline.*