Reliance on Internet Highlights the Need for Out-of-Band Authentication from Boloro

We are all stuck at home and we are all living and working online. Virtually everything that we do is virtual, including online banking, digital payments and eCommerce, meaning we are all traveling non-stop on an information superhighway that was never built for safety and security. The Internet was built for mass dissemination of information and never designed for secure transactions and other risky activity, allowing fraudsters to run rampant with identity theft. We see stories every day about email being hacked and Operating Systems being subjected to malware, making online activity inherently vulnerable to fraud. Our increased reliance on online activity during the COVID19 pandemic is highlighting these long-standing problems. SIM Swaps, email hacks, malware, man-in-the-middle attacks and other forms of fraud are all rising dramatically. The decentralization of customer support desks may be contributing to the ability of fraudsters to wreak havoc on security.

What can be done to put real security in the hands of consumers?

As activity on the Internet and Operating System is increasingly becoming easy prey to sophisticated fraudsters who routinely exploit the single point of failure, we need a new approach to security that avoids the Internet and Operating System. Security should not only be multi-factor, but multi-channel, eliminating the vulnerabilities of a single point of failure. So-called “in app security” is still touching the inherently vulnerable Internet, meaning consumers who use it are still putting all of their eggs in an unstable basket. Out-of-band security is the way to go. When activity is on one channel, authentication should be on a separate channel, providing an independent lock-and-key that cannot be intercepted and compromised.

At a time when the world is increasingly becoming aware of the inherent vulnerabilities of the Internet and Operating System, we are also seeing how dangerous it can be to touch a public Point of Sale device, ATM keypad, finger scanner, iris scanner or anything that could spread the coronavirus. During the best of times, we should not be passing germs to each other by all touching public devices. During a global pandemic of this magnitude, the importance of keeping your hands to yourself is constantly being emphasized. Social distancing is much more achievable when we can each do everything safely and securely on our own personal mobile handset, avoiding the need to touch a public device. Boloro's multi-factor and multi-channel security on your personal mobile handset is the answer.

Boloro Authentication is both multi-factor (the physical handset that you possess and memorized secret that you know) and multi-channel (separating the authentication channel from the activity channel). Boloro Authentication has been approved by the Global Association of Mobile Carriers (GSMA) and meets the worldwide definitions of Secure Customer Authentication. In addition, Boloro does not require any personal biometric data, providing real security that is also in compliance with global data protection and privacy regulations. Boloro is working with Mobile Network Operators in India, Africa, the Middle East and other markets to leverage the secure signaling channel, push USSD or network initiated USSD, to separate the authentication from the activity itself. We are now also actively bringing our solution to the Americas, where it is ideal for numerous use cases, including online banking, digital payments and the prevention of card-not-present fraud, as well as logins for email, social media, and access to data.

With Boloro, all activities are conducted safely and securely on the personal mobile handset, eliminating sole reliance on the Internet and eliminating physical contact with a public device or screen. Boloro is compatible with all mobile phones, including smartphones and feature phones, and easily deployed via APIs for local hosting and / or cloud-based hosting. Use cases include online banking, digital payments and e Commerce, as well as the avoidance of touching public Point of Sale machines, ATM keypads, finger scanners and other public devices by putting all activities safely and securely on the personal mobile handset.

Boloro is ready to work with you to make the world a safer and more secure place!

We look forward to hearing from you.
Sincerely,
Karl P. Kilb III
CEO
Karl.Kilb@Boloro.com