OPINION

SECURING THE MOBILE, KEY TO YOUR DIGITAL EXPERIENCES

A digital, mobile-first world has implications for service providers, too. **Irfan Abubaid**, VP of messaging and digital services, HGC Global Communications, explains

Irfan Abubaid, VP of messaging and digital services, HGC Global Communications

Gone are the days when our lives were dependent on bricks and mortar. More and more of our exchanges and transactions are being digitalised. However, as people and businesses become tech-first, new challenges are being encountered.

Most services need a password, and that password should ideally be unique to a given site/platform. Still, for individual users such as myself, it is difficult to remember unique passwords for every site or service I sign up to. This creates a security challenge, which is exploited by fraudsters.

For every hack and subsequent data theft of personal data, end users' credentials are being sold on the dark web to allow other criminals to use this data to gain access to other services that a given user may have.

This has serious implications for the individuals affected, and for the businesses that serve them. Loss of revenue, reputation, customer trust or loyalty – as well as fines for breaches – are just some of the negative consequences for businesses. Taking online payments, for instance, merchant losses as a result of online payment fraud are estimated to exceed US$206 billion cumulatively for the period between 2021 and 2025, according to Juniper Research.

The value grows to staggering amounts as more verticals are added. In this digital world, it does not matter if a business is in finance, gaming, commerce or e-health; every organisation needs to defend itself by identifying vulnerable loopholes. It is increasingly important for businesses to implement advanced ways to tackle new and complex attacks such as impersonation scams, scary intrusions, phishing, malware distribution, or identity fraud, which lead to data leakage.

> ***In this mobile-first scenario, trusted partners are essential to support such security layers***
>
> **Irfan Abubaid,**
> **VP of messaging and digital services,**
> **HGC Global Communications**

The shift to digital has transformed banking, as high-street branches are replaced by mobile apps and online assistants. This change has meant that both younger and older generations are now increasingly being asked to bank online, which means they risk becoming targets for fraudsters. As the demand for and usage of real-time bank transactions continue to increase, it is critical that enterprises deliver non-intrusive and seamless ways of engaging, verifying and protecting customers and their user experience.

The mobile device is increasingly being used for these transactions, as well as a means to secure the transactions themselves with two-factor authentication. The reasons for this development are clear:

- Users typically carry their mobiles with them at all times, so it is an ideal platform/key;
- There are a lot of mobile subscribers today – more than five billion;
- More secure solutions are needed.

In this mobile-first scenario, trusted partners are essential to support such security layers. Mobile intelligence services give service providers across many verticals access to mobile operator data conveniently, hence enhancing security and the online service user experience.

For example, the last SIM change time stamp can be used to assess risk of account takeover before sending the SMS OTP. And with "number verify", the service provider can check if the phone number of the mobile accessing the service is the same as the phone number on file through an API call, rather than SMS OTP, thus reducing user friction. Number verify has been very successful in several countries, including China, with more than a billion daily transactions across the main operators.

Ultimately, for operators with robust communications portfolios, such as mobile intelligence services, companies can enhance their offerings with optimised security and frictionless user experience. Through connecting to API platforms, access to multiple mobile intelligence data from several different mobile network operators is made easier.

The shift to digital channels is here to stay, and we believe that partner ecosystem is highly effective in delivering seamless online experiences. That is why we continue to connect service providers with mobile network operators' capabilities and data; together, we help deliver simpler and more secure user journeys.