Recently, Vodafone and TalkTalk suffered high profile data breaches making thousands of customers vulnerable to phishing attacks and fraud. Leakage of user credentials and personal information not only affects users, but also online retailers who are impacted by chargebacks on fraudulent transactions.

No doubt, security for online payments will be under the microscope once again in 2016. As new technologies continue to disrupt mobile payments and financial institutions and payment service providers still remain unsure of their responsibilities when it comes to fraud prevention, the time has come for the mobile commerce industry to reconsider its approach to security.

Shoppers vulnerable to fraud
With over 50% of all ecommerce internet traffic coming from mobile devices according to Shopify, users will be as vulnerable as ever to the possibility of fraud. In addition, a considerable percentage of shopping is now done on the move leading online retailers to make the shopping process, including checkout, quicker and user friendly.

So how can retailers, banks and payment service providers work together to strike an effective balance between creating a secure environment for users making online payments on their mobile devices and maintaining a good user experience, a degradation in which would inevitably contribute to a decline in check-out conversions?

Gartner has outlined three categories of applications and services that help enterprises secure m-commerce through user authentication: mobile app security; mobile environment security; and mobile-friendly user authentication. While online retailers can take some measures in terms of the first two categories, they are limited in terms of strongly enforcing these; for instance they wouldn’t want to restrict usage to specific browsers or attempt to manage users’ devices. This leaves mobile-friendly user authentication as the main category for mobile commerce vendors to focus their security efforts on.

Unfortunately, traditional login and password-based authentication is too outdated to cope with modern day security threats, and is a hindrance to users in terms of the experience on mobile. Such static passwords leave the door wide open for hackers as their fraudulent ambitions rely greatly on human nature; we all have too many passwords to keep track of, and either make simple ones or reuse the same password for multiple accounts.

**Strong forms of authentication**

Phone number verification, on the other hand, is a stronger form of authentication and provides a better user experience on mobile devices making it ideal for mobile commerce.

So, how does phone number verification work? Essentially, it is based on using a phone number as the user identity. Phone numbers are relatively expensive and time-consuming to fake, everyone has a number which is personal to them and they tend to retain for a long period of time and no additional hardware is required (which makes using mobile as a security tool more affordable). Phone number-based authentication differs from static passwords as it involves sending a one-time password (OTP) to a user via a separate means of communication (usually a text message or a voice call) which only the user has access to. And this one-time password expires within a short period of time.

For increased security, phone numbers can be combined with device identifiers to ensure that users have access to not only the phone number they use as identifiers but also the mobile devices they have registered for use with the application. In this scenario, push notifications can be used to send verification codes that are automatically consumed by the mobile commerce application to provide a seamless experience for users.

Should mobile security be a priority, even if at the expense of the customer experience? With only 67% of banks under the impression that providing security is a mandatory requirement and 48% of financial institutions admitting they act to mitigate the situation rather than provide a solution according to Kaspersky, the truth is that until law intervenes, mobile commerce vendors must take some of the responsibility for protecting themselves from chargebacks and their users from breach of personal information.

*This post originally appeared on SmartChimps.*
First Name

Last Name

Email Address

Phone Number

Are you a Developer?

Company Name

Select Country

Product of Interest

Existing traffic to switch?

Traffic Volume Monthly (Optional)

Message (optional)