bizcommunity

The challenge of e-commerce transactions on a mobile device

By Leigh Andrews 27 Jan 2015

Do you have an antivirus product on your mobile phone? If not, best you invest in one in order t protect against mobile fraud, as mobile payments and card-not-present retail go on the rise...

On Monday, 26 January, PayU held a seminar on digital security and fraud management at the Naspers building in Cape Town. The venue was fitting as PayU is a subsidiary of Naspers. Speakers included Andr Henwood, CEO of Foregenix; as well as Mustapha Zaoulini, CEO of PayU EMEA; and Bryce Therrold, lea of Visa's sub-Saharan African Country Risk Management team.

Topics included being secure with Visa, PCI and online security, the PASA security landscape and a view security in South Africa, as well as PayU's fraud management systems and new innovations from PayU.

What exactly is PayU and why is 3D Secure important?

Simply put, PayU enables e-commerce by offering secure and reliable online payment services to South African businesses and consumers. The seminar kicked off with an introduction on 3D Secure and PC compliance, with Zaoulini giving a high level view of trends from a global and PayU perspective. He mentioned that 18 countries have integrated under PayU, and that the company has evolved from just a gateway or business-to-business platform to its current broader focus on the end user being able to transa anywhere, at any time. He said that in 2015, PayU's user experience or UX will be enhanced to be more responsive and take into account trends like the Internet of Things or IoT and taking online offline.

Mustapha Zaoulini, CEO of PayU EMEA

According to Zaoulini, 2014 saw a rise in pre-ordering products online, which has security implications for the merchant and consumer alike. We also saw Apple launch the iPhone 6, and other technology being adopted that's set to effectively change behaviours across the market. Wearables becoming more popula too, which is an exciting shift. With all of this as a background, Zaoulini spoke of the trends we can expect from 2015.

Six trends for 2015 that'll change the face of mobile transactions

The first of these is **consumer digital ID** or biometrics. For example, think of how facial recognition, fingerprints and voice recognition are already in use at most local banks. Next is **relevance**, with Zaoulini

saying he expects Uber will be a strong player in the payment space soon as it's collecting lots of data on users, which means it can offer personalised loyalty. This links to the topic of **stored credentials**, which refers to the loyalty points we collect across our different accounts. At the heart of it, it's a battle of the brands, with consumers having to decide which brand they trust the most to store their details, whether it's Facebook, Google or retail, merchants need to be cognisant of this and build solutions around it. Zaoulini's next point is that of **virtual or crypto currency** like Bitcoin. The topic was even discussed in a positive lig in Davos last week, so it's definitely relevant and on top of the global agenda. Possibly the most impactful trend listed by Zaoulini is that of **mobile or micro payment**, which is where merchants enable consumers transact with small amounts across multiple channels. His final trend to watch for was that of **innovative creditworthiness**, which he likened to the idea of having Uber as your financial credit provider and having linked to social media purchasing and prepaying. There are already lots of players in this space locally, as well as in Nigeria and Kenya, so expect this to become more mainstream soon as mobile payment goes mass market.

The biggest challenge of implementing mobile payment...

Unfortunately it's not all plainsailing as there are big challenges around acceptance and incentivisation. The challenge is twofold as you need to make the mobile process convenient for the merchants, while also making it an attractive option for the consumer to adapt to. In order for this to be successful, we need to increase our efforts at education on the topic and build confidence in all involved.

This is crucial because as technology is evolving, so is cybercrime. This means your antivirus program ma not be enough to protect your funds, especially if it's only activated on your PC and not on your mobile, where you make payments. This speaks of the common need to protect your private data as a consumer.

© Scanrail – 123RF.com

Keeping with the topic, Johan Dekker, COO of PayU spoke briefly of 3D Secure as a fraud management system. As a merchant, he says it's a good idea to step into your consumer's shoes and apply common sense - if it sounds too good to be true, it probably is. Use this mindset to educate your users as well as y employees, because while the online space is growing in leaps and bounds, awareness just isn't on the same growth path and people are still wary of sharing their details online, especially through mobile. His fir piece of advice was to remember that each click you can eliminate for the consumer strengthens the chan that they will actually complete the transaction. Click here for Dekker's 5 things to be most aware of and 10 ways to walk away from becoming a victim of fraud.

Learn from the PC Forensics Investigator's insights...

Next, Henwood spoke of being a 'PC Forensics Investigator'. He says the onus is on the merchants to sto the data leak in the first place to minimise mobile fraud at the check-out phase. Sadly, he says the same-o vulnerabilities in the e-commerce space are being violated through SQL injection attacks, which are alread over a decade years old - so anyone can come in, literally query the database and access the information. Remote access is also a risk. All this points to the fact that hackers don't even have to use fancy, hard cor exploits to get in, it's more about being increasingly sophisticated at extracting information as fast as they can. Henwood cautions that until the whole world goes 3D Secure, there will be a risk of fraud. Even worse he says the average length of time taken to discover your website's security has been breached is 270 da - and sometimes you even have hackers hacking the original hacker. This points to the importance of stori and monitoring logs daily, such as security and remote access, as well as sudden patches or upgrades tha you don't remember installing onto the website. Henwood says that regular site backups are also crucial. H ended with a stern warning to merchants that simply having antivirus installed is not enough as these hacks are just not going away.

Thorrold was the last speaker at the podium for the morning. He says not a lot of merchants actually like 3I Secure, and that it's important to know what your cardholders feel. You need to research, understand, trac and predict spend from your cardholders in order to prevent future theft by monitoring their spend and keeping an eye out for anomalies. On the plus side, he says research shows consumers are now paying more attention to their mobile handsets during the transaction process, and they acknowledge that while having to enter their credit card's CVV2 digits for each transaction is annoying, it's a good way to minimise fraud as it's proof that they're actually holding the credit card in front of them.

All in all a thought-provoking morning. Visit Dropbox to view all the PDF slides of the presentation.

ABOUT LEIGH ANDREWS

Leigh Andrews AKA the #MilkshakeQueen, is former Editor-in-Chief: Marketing & Media at Bizcommunity.com, with a passion for issues of inclusion, belonging, and of course, gourmet and drinks! Now follow her travel adventures on YouTube @MidlifeMeander.
View my profile and articles...