AMERICAN MARKETER

Business at its best

COLUMNS

Mobile security: the elephant in the room

January 7, 2011

By Gary Schwartz

In 2010, we heard about and saw the huge potential for mobile commerce.

ABI Research forecast that for 2010 the North American sales of physical goods purchased via a mobile device was more than $1 billion, up 33 per cent from its 2009 forecast of $750 million. PayPal Mobile traffic last year was indicative: up 300 percent.

But is there an elephant in the room? Is mobile commerce fraught with security concerns?

U.S. research in October 2010 study found that two-thirds of 30 applications selected from the most popular titles on the Android Market "used sensitive data suspiciously," transmitting data including location, device IMEI and, in some cases, the phone number and SIM card serial number (ICCID), for purposes not explicitly clear to the end user.

According to a Juniper Report in the same month, "More than 76 percent of consumers surveyed use their smartphones or tablets to access sensitive personal or business information, including 51 percent to enter or modify pass words; 43 percent to access banking or credit card statements; 30 percent to access utility bills; 20 percent to share financial information such as credit card numbers; 18 percent to access employer's proprietary information; 17 percent to access medical records; and 16 percent to share social security numbers."

Tsks about risks

The modern mobile phone is a digital device as security-challenged as a desktop PC.

We have already seen, in a variety of countries, concerns expressed by governments and media about the risk of unauthorized access to private user data such as location, profile and banking information.

The reality is that the industry needs to seriously look at developing security standards immediately to maintain the growth and levels of consumer and retail confidence.

Ultimately, to get the shopper to be comfortable on new technology, they have to be confident in the security of the device. There is no time to be complacent.

At the MEF Americas 2010 conference in Miami, MEF announced phase two of its mobile commerce work, taking a deep dive into consumer and merchant confidence in using the mobile device to enable commerce.

Keith Enright, chief privacy officer at Macy's Inc. and a keynoter at the MEF Americas show, is one of the few voices openly discussing mobile consumer information risk management.

"The mobile channel and mobile payment mechanisms can be secured like any other channel, not perfectly, but relative to risk," Mr. Enright said. "However, questioning whether mobile security is the same as or different than online security misses the point."

For Mr. Enright, digital security is the ability to establish effective controls based on a thorough understanding of strengths and vulnerabilities.

"The analysis online or in a mobile environment would be similar, but the most effective controls may differ," he said.

So what are these "effective controls" and how do we know we are doing a good job addressing the vulnerabilities of the mobile medium?

"The mobile channel and mobile payment mechanisms can be secured, like any other channel, not perfectly, but adequately relative to risk," Mr. Enright said.

"Just as the World Wide Web evolved far past the goals of its conception, uses and applications of mobile technology are outpacing effective controls to mitigate known and anticipated risks," he said.

"With this in mind, the mobile industry could benefit from collaborative efforts to take existing, well-established security risk assessment methodologies and standards, adapt them as appropriate and apply them consistently to new and expanded uses of mobile technology."

Old drumbeat

As we explore how linking payment and location effects privacy and security for the shopper, some retail executives are sounding the alarm.

"There are going to be some symbolic lynchings of a few mobile commerce players by regulators before we settle on best practices in this space," cautioned one retail executive I spoke with recently.

With legacy bank cards, financial institutions are dealing with security and fraud by embedding "Chip and PIN" in the plastic replacing the magnetic stripe-based systems.

The banking world calls these features "secure elements," or SE.

The first mobile contactless payment pilot started in 2003, and was followed by many pilots.

The industry is looking for ways to secure mobile payments at a comparable level to plastic. Eight years later, there is still limited SE on the handset.

Shoppers need a mass-retail solution to begin comfortably waving their phones to make purchases.

There are always going to be vulnerabilities, and the mobile payments industry needs to understand that it has to minimize the risks and explain how the risks have been mitigated.

Banks have always shown that they have a strong stomach for payment risk on new platforms.

ATMs needed to accommodate teller-not-present transactions. Catalog phone orders needed accommodate card-not-present transactions.

As remote payment access moved online and now into the mobile space, so have risk and vulnerabilities increased.

Risk has not only increased for the shopper, but for the entire payment value chain.

The retail and banking communities again seem to be waiting for legislation to mandate standards. X9.org is working away at mobile compliance standards this year. This is a good sign.

Is this the Internet all over again? Will mobile wait for the same drums to beat? I certainly hope not.

Gary Schwartz is CEO of Impact Mobile, Toronto, and chair of MEF North America. Reach him at gary.schwartz@impactmobile.com.