



2015 Mobile Payment Security: Perceptions and Behaviors

There's no question about it: mobile payments are convenient—and as we can all probably attest, convenience can be compelling when it comes to influencing consumer behavior and driving consumer interest. Put simply, **convenience has power**. Consider that quite a few business transformations and game-changing paradigm shifts were historically driven by enhanced convenience: TV dinners, household appliances and ATMs, for example. More recent examples include e-commerce, online banking and streaming movies.

Consumers want convenience. It follows logically, then, that new business models embracing convenience are likely to get traction. As one might expect, we have seen areas in which mobile payment adoption has bloomed. In Asia for example, according to a 2014 Nielsen report¹, e-wallets and mobile payment are already in active use and are the preferred payment vehicle for many consumers' routine spending. But in other regions (North America, Europe, the Middle-East), adoption hasn't been as strong. The same Nielsen survey found that only 38% of those in Europe and 41% of those in North America would shop online with a mobile device if the card could be stored safely.

When a new offering that provides consumers with significant convenience isn't widely adopted as quickly as expected, it's useful to examine the underlying reasons why. For those of us in the ISACA community—in

other words, those of us with a vested interest in managing risk and maximizing value for our organizations—it's particularly important. Why? A host of reasons: it impacts us personally as we weigh the risk/rewards of embracing mobile payments in our personal lives and it impacts us professionally as we evaluate the use of mobile payments for business activities (either offering the option to our customers or enabling it for our employees).

To attempt to quantify and qualify the underlying forces at work in the mobile payments space—specifically the risk and value tradeoffs that are driving both personal and corporate adoption—ISACA surveyed more than 900 cybersecurity experts around the world about their use and perception of mobile payments. What we found

People using mobile payments need to educate themselves so they are making informed choices. You need to know your options, choose an acceptable level of risk, and put a value on your personal information. The best tactic is awareness. Embrace and educate about new services and technologies.



CHRISTOS DIMITRIADIS
Ph.D., CISA, CISM, CRISC,
International President of
ISACA and Group Director
of Information Security for
INTRALOT

¹ February 2014, "Global Payment Gateways of the Future," Nielsen

87% of those surveyed expected to see an increase in mobile-payment data breaches over the next **12 months**.

helps shine the light on the underlying dynamics at work.

Security and Risk Concerns

First and foremost, we found that many of those we surveyed say mobile payment technologies have a security and risk element associated with their use. When ISACA first published our initial research guidance on mobile payments in 2011, we noted that while the business benefits were potentially significant, some security and risk challenges would need to be worked through as the technologies mature. The market reception has borne this out. Specifically, only 23% of those we surveyed say transactions using mobile payment methodologies are secure; all other payment instruments we asked about (cash, credit cards, debit cards, checks, and money order) had double-digit higher results. Additionally, 87% of those surveyed expected to see an increase in mobile-payment data breaches over the next 12 months.

In terms of specific security concerns related to mobile payment, the most significant were: use of public WiFi on a payment-enabled device (26%), lost/stolen devices (21%), and phishing/smishing (i.e., phishing conducted over SMS) (18%) topped the list of concerns.

One data point that stands out from the survey is this: while many of the

respondents lack confidence in the security aspects of mobile payments, that lack of confidence is not entirely deterring shopping behavior using mobile. Specifically, 42% of the cybersecurity professionals surveyed had used a mobile payment platform to make a purchase.

Addressing the Challenges

Since many people are using mobile payment regardless of their concerns about security, the question becomes: what can individuals do to help ensure the security of their information, and what can business do to help minimize the risks as mobile payment technologies continue to develop, spread and increase in use?

We asked exactly that: what is the most important action that consumers can take to improve the security of mobile payments? By far, respondents indicated that the use of two-factor authentication (using multiple ways to confirm your identity) on the mobile devices was most important (66%); this was significantly ahead of the other approaches we asked about such as use of a limited-duration code (18%) and phone-based security applications (9%). So, for individuals, enabling built-in two factor options on their device might be advantageous, and enterprises may consider incorporating this into their policy about mobile device use.

Mobile payments represent the latest frontier for the ongoing choice we all make to balance security and privacy risk and convenience. ISACA members, who are some of the most cyber-aware professionals in the world, are using mobile payments while simultaneously identifying and contemplating their potential security risks. This shows that fear of identity theft or a data breach is not slowing down adoption—and it shouldn't—as long as risk is properly managed and effective and appropriate security features are in place.



JOHN PIRONTI
CISA, CISM, CGEIT, CRISC,
Risk Advisor with ISACA and
President of IP Architects

Early Education Is Key

The study also asked about the implications for younger consumers and the practices most beneficial to them—i.e., what parents can do to protect children who may either have access to a mobile device or occasional use of a parent’s or household device. First of all, it was clear that education about mobile security at a fairly early age is a priority. Nearly three-quarters (73%) of respondents indicated that education about mobile device security should happen before youngsters are 13 years old, and nearly half (46%) said that

14-17 is the “right age” for them to be given their own device. The implication? Children should be taught about mobile phone security before they have one. Good advice.

The survey also examined the top steps adults should take to safeguard the security of a child’s smartphone. Requiring a PIN or password for access was in the top slot (72%), while parental control software (58%) came in second. Tied for third were remote wipe (53%) and general (i.e., non-parental-control specific) mobile security software (53%).

Conclusion

Mobile payments are only growing, and ISACA advocates an “embrace and educate” approach. Understanding the security risks, as well as the specific steps that we can take to mitigate those risks, is essential to being prepared for them and protecting our organizations, our families and ourselves. By managing the related cyber risks, we can more fully take advantage of the benefits that innovative technologies like mobile payment can deliver.

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.



3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

PHONE: +1.847.253.1545

FAX: +1.847.253.1443

EMAIL: info@isaca.org

www.isaca.org

**Participate in the ISACA
Knowledge Center:**

www.isaca.org/knowledge-center

Follow ISACA on Twitter:

www.twitter.com/ISACANews

Join ISACA on LinkedIn:

www.linkd.in/ISACAOOfficial

Like ISACA on Facebook:

www.facebook.com/ISACAHQ