Betting the farm on untested tech

By Jonas Thulin, Security Consultant at Fortinet

While a plethora of new payment solutions are coming to market, businesses should be cautious about moving to new solutions just for the sake of it.

Customers are driving a great deal of change in how transactions are carried out, with the younger generation of consumers in particular demanding newer, faster and more convenient ways of transacting, using a variety of electronic channels. Some of these channels are proving highly successful: thanks to developments such as mobile banking and online banking, the unbanked are becoming banked and consumers have greater convenience than ever before.

But with a continually growing list of options for making and receiving payments, businesses need to be cautious about trying to accommodate every new payment channel and app that emerges. Rushing to adopt immature technology just because it is ‘cool’ could end up costing business dearly.

The simple fact is that security is a risk around untested, immature technology. Mobile app developers generally make security their secondary concern; mobile devices are usually unsecured, and mobile browsers and networks are often not secure. Near Field and Bluetooth payments pose eavesdropping risks. Even in environments where network and system security is a focus, the end user presents a vulnerability, because social engineering is still a highly successful method of breaching security. In an environment fraught with risk, adding new, untested payment solutions to the mix will add to the complexity of the environment that must be secured.

Any business offering payments via a new channel will need to create an environment of trust, and will also have to be clear about recourse and compensation in the event of fraud taking place during the transaction. If credit card fraud occurs, the bank will likely cover the costs if the user can prove he or she took measures to prevent fraud, but the measures that should be taken to prevent fraud in mobile payments are not as clear. Who will be accountable? What security measures should the user be expected to take to protect the device and safeguard the transaction?

The business offering greater convenience through new payment channels might have to be willing to ‘carry the can’ in the event of fraud, or it will have to educate its consumers about the risks involved in the transaction – which could deter potential customers. Failure to warn customers and an unwillingness to cover their costs in the event of fraud could prove costly in terms of reputational damage.

There are also hidden costs involved in many new electronic payment tools such as mobile app-based systems: they can take a few seconds longer to process than credit card payments. For a busy retailer, every second’s delay at the till adds to the cost of doing business. So businesses embracing new payment channels would have to carefully weigh up the risks and benefits of the new channels.

The cashless payment environment is a challenge. It’s bleeding edge and much of the technology is very immature, so it will take a level of boldness for a business to enter this world.

/ENDS.