Digital pick pocketing: An industry born from scaremongering

John Elliott of Consult Hyperion investigates

Ever since the banks and the financial services industry started rolling out contactless payment cards, and merchants adopted contactless payment terminals, a new security industry has grown warning us of the threat of having your card data read. In fact, you've probably seen the articles or YouTube videos that claim that your new contactless payment card details can be read by an attacker while your card is in your pocket, perhaps closely followed by a sales pitch for some sort of foil sleeve which can prevent your card from being read. (http://wreg.com/2012/01/10/electronic-pickpocketing-goes-viral/).

Today, rather than only being used to buy fast food and transport ticketing, contactless cards are also starting to be accepted in book shops and stationers, and latest figures from UK Cards indicate that, in the UK, there are currently more than 20 million contactless credit or debit cards issued and 80 thousand readers where they can be used at merchants. HSBC has been the latest bank to announce that it will start replacing customer debit cards with contactless cards. But, interestingly, they are allowing customers to opt out if they would rather not have the new contactless technology in their wallets. Do we read into this that even they, one of the world's biggest banks have bought in to some extent, to the scaremongering stories in the media and on the web and are knowingly putting customers at risk? I think not, so let's investigate and see if there is a threat, and if it really is any greater than what already exists from using payment cards?

What can be read?

When a card conducts a transaction with a card reader, the reader is the master and the card is the slave. So, to some extent, the card will do what it is told, and this involves giving up some information about the card. The necessary specifications are easily obtained and the kit is cheap, so it is not hard to make your own contactless payment card reader to obtain the free-read data from all contactless cards to which you can get close enough (less than 10 cm is what the standard says)

By comparing what can be read from a contactless chip, with what can be easily obtained by a visual inspection of the card i.e. if you lost your card or it was stolen and used for fraud, we can determine how big the threat is. The Primary Account Number or PAN, which is the long number across the middle of the card which identifies the issuing bank and the account which will be used to ultimately pay, can be read visually and via contactless. It's the same scenario too for the card's expiry date. However, the 3 digit security code on the back of the card used mainly for online transactions and the cardholder name (apart from some very early contactless cards), cannot be read via the contactless chip, but can be obtained of course by visually reading these card details.

So, how scary is that?

Well, the short answer is, that's not very scary at all, and the threat is much greater should you physically lose your card and a fraudster uses it, than if information was obtained over the

contactless interface. But the stories continue to circulate about how unsafe these new contactless cards are, so the big question remains: how much do contactless cardholders really need to worry about 'sniffing'? According to the payment scheme rules, cardholders are protected against both of these threats – provided that they do not break the rules (such as revealing their PIN). After all, debit and credit card transactions of all types come with their own risks, just as walking down the street with a wallet full of cash can open you up to a risk of being mugged.

As with any new payment technology, much like when cards were introduced, you're being offered more convenience, but perhaps at slightly more risk. So the general rule of thumb with contactless cards, and with a 'normal' card for that matter, is to keep your card safe and close by and don't reveal your PIN to anyone. However, if you still have concerns about what can be read from your contactless payment card in your pocket (i.e. your card number and name), then I suggest that you simply wrap it in a piece of kitchen foil, since that alone will prevent any reader from reading it unless the foil is removed. That should give you total peace of mind – as well as a much better alternative to the card shields vendors cashing in on consumer fear and hype who will no doubt continue to fuel the misconception that contactless cards are not safe.