Why we do dumb things on smartphones

February 28 2014, by Nik Thompson

Think of the risks before scanning that QR code. Credit: Flickr/ scott_bl8ke, CC BY-NC-SA

Imagine this: you're surfing the web while out at lunch. You decide to buy concert tickets, so to save having to put your sandwich down you ask a passer-by to log in to the ticketing website for you.

As unrealistic as this scenario sounds, users regularly do that when they scan, click and navigate to potentially untrusted internet resources with only a machine-readable matrix – a QR code – to lead the way.

QR codes are matrix barcodes created by Toyota subsidiary Denso-Wave in 1994 to identify automotive components. Physically they are similar to traditional barcodes used on product packaging.

The matrix configuration allows for a denser data format which stores thousands of characters, rather than the 20 digits that product packaging barcodes hold.

Marketers and advertisers have embraced QR codes as they provide a link between the physical and the digital worlds. This simple printed shape can be created for free and can provide a link to an associated website when users scan the code with their smartphone.

Where do the risks arise?

Firstly, the non-human readable nature of the QR code is significant because it breaks the "read first – click later" behaviour that we have tried to encourage for any online transactions. We can get some idea of what a website will be, before visiting it, by reading the URL. In many cases, by the time the user has pointed their phone at the QR code, the website has already been accessed and started loading.

A study by researchers at Murdoch University last year found that some of the most popular QR scanning smartphone apps do not provide enough feedback or status information to users before visiting a web link. This means that even tech-savvy users are at risk in an era where speed or ease of access is somehow a higher priority than secure functionality.

The bigger risk factor here is how threats are perceived by users. Most security research focuses on technical or architectural issues. Human factors are often overlooked, even though they may pose the most fundamental and severe threats.

Recent history has shown just how rapidly technology can progress. But with rapid uptake (such as smartphone usage) there is an inherent danger that corresponding human behavioural and attitudinal changes may not

occur. In nature, new and unfamiliar environments may well be the most risky, and the digital landscape is no exception.

Just another computer

Many users don't appreciate that a smartphone is just another computer; albeit with a smaller screen and no keyboard. They are generally familiar with the dangers associated with accessing untrusted websites from their home PC but they don't apply this same advice when they are scanning a barcode with their smartphone.

The disparity in security behaviours is quite striking – a recent study of 458 smartphone users revealed 85.8% use security software on their PC compared to just 24.5% on their smartphone. With sales of tablets increasing and smartphones overtaking desktop PCs, this is an arena which will soon receive a great deal of attention (both good and bad) from software developers.

If we look to the psychology literature for help, then Protection Motivation Theory may be one way of explaining how users perceive and respond to threats from their environment.

The theory suggests that the motivation to protect oneself from a threat is related to the belief that the individual is personally vulnerable to the threat, that the threat is severe and that the response will be effective in preventing the threat.

Wise up on smartphone use

Mistaken beliefs such as "smartphones are not susceptible to security problems like desktop PCs" must be dispelled as they directly influence the behaviour that a user may exhibit.

The good news is that this understanding is a step towards a more comprehensive smartphone security model, taking into account human as well as technological risk factors. Protection Motivation Theory also suggests that if users can be shown that they're in a position to respond effectively to these threats, then behavioural change is more likely.

The QR code risk that sparked this whole discussion is just a symptom of a more systemic issue of the security behaviours of smartphone users as people use them more for things such as online banking, buying tickets and other financial transactions.

Judging from the current trends, just like any other business that targets the biggest user base, criminals are no exception. So as the use of smartphones as a mainstream computing platform grows, so will the extent and severity of malware and attacks. But unlike the technical issues which can be cured with a software patch, behavioural change is much harder to initiate.

At the individual level, there is a strong behavioural influence exerted by the social environment, and a critical mass of change may be required before mainstream effects are seen.

These may be manifest as stronger screening of apps for potential risks and traps, more community trust ratings within app stores and the use of on-device security software, linked to publicly shared threat databases.

Perhaps more effective still, is awareness that mobile security is a personally relevant issue that can be addressed with no cost or impact on day-to-day use of their smartphone.

The predominant attitude to security is reactive in nature, but by turning this around, users can take control of their own mobile security.