Don’t Expose Your QR Codes

On the 16th of January, the Tasmanian Racing Club Inc made a post on their official facebook page about giving away 10 tickets to the upcoming hobart cup. That post had a photo attached (visible above) in which two of the ten tickets have their QR codes showing.

The Problem

These visible QR codes appear to contain information proving that they are in fact real tickets that someone could copy and use to get into the event without paying.

QR codes are just text encoded into a picture that computers can easily read from a photo. The contents of the first QR code (front most ticket) is “hobart-cup-2018-151” and “hobart-cup-2018-156” is the contents of the 6th ticket. From this it can be deduced that the numbering is sequential and therefore the tickets in the photos contain the numbers 151 to 160 in their QR codes. The numbering probably doesn’t stop at 160, so numbers above that could be used to spoof other tickets.

The Solution

- Don’t have the QR codes visible in any photos.
- The number appended to “hobart-cup-2018-” should be random and not sequential in any way. This is to make sure that someone with one ticket cannot easily guess the QR code of the next ticket.

Disclaimer

I do not intend to use this exploit in any way. This is me, Liam Kinne, disclosing this exploit privately so the Tasmanian Racing Club Inc are aware.