MIDNIGHT CLUB

The story of the fastest street racers the world has ever seen

ITMAM BASHAR

When people hear about street racers they tend to visualise a group of people driving recklessly and performing burnouts - akin to scenes from the Fast and Furious movies. What they don't picture is a well-to-do, respectable, wealthy businessman as a part of an elite and highly selective club - with a strict code of ethics and just one goal: "to build and race the fastest car's the world has ever seen".

The Bayshore route of Japan is a stretch of coastal highway that connects Tokyo to Yokohama. While it may not look like much, it is the spiritual home of Japanese street racing. To the locals, it's known as "The Wangan". Wangan is loved by street racers due to its long straight sections and relative emptiness at night, where for decades it was used by the racers to push their cars to the limit. As the streets got busier and more heavily policed, racing in Wangan died down but for years to come, stories will be told about one particular group of racers - Midnight Club.

In 1987, during Japan's golden era of tuning, the secret society of highly skilled drivers was founded. A large number of different street racing gangs existed in Japan at the time, but there were a few key things that set the Midnight Club apart. For starters, they were highly selective. To become a member you have to be an exceptionally talented driver with a suitably fast car. Plus, you have to be an apprentice for a year and attend every single meeting during that time.

That wasn't as easy as it sounds because the club members were wanted criminals, with the meeting locations being shared via coded messages in the classified ads section of local newspapers. Surprisingly only 10% of applicants were ever accepted to the club and numbers rarely exceeded 30 members. They were also highly protective of their club's name, many aspiring young racers fraudulently decorated their cars with the iconic midnight decal but often woke up to find their car vandalised and the sticker removed.

In the Midnight Club, races were not about acceleration or cornering ability like the Kanjozoku. Instead, they were about one simple thing: top speed. A club member once quoted, "Drifting is for the weak. We only do maximum velocity". The races are won only by reaching the finishing line first or getting so far ahead of your opponents that they can no longer see your taillights.

Simply to be considered for membership, the car had to sit on 260km/h comfortably. But in races, the cars regularly exceeded 300km/h and even 330km/h. Keep in mind that this took place in the 1980s. That's why so few members of the Midnight Club were ever arrested, owing to Japanese police cars of the period being limited by law to 170km/h.

It's obvious that the cars weren't like average street racer cars, and weren't required to just have an enormous top speed. In races, they had to maintain that top speed for up to 15 minutes, indicating that they also had to be reliable and well-built. This resulted in members being wealthy business owners spending millions of dollars building some of the fastest and the most incredible cars the world has ever seen. The most legendary member's car was the Ishida Specials 930 Porsche 911 Turbo which is fondly known as 'The Widowmaker' or 'The Blackbird'. The owner has been rumoured to spend the modern equivalent of over US $2 million modifying the car, improving every measurable aspect of the performance and increasing its power up to 700Bhp. That is more than a brand new 911 GT2 Rs, in an RWD car built in the 1980s.

The most unique thing about the club was not the cars or the skilled drivers but the code of ethics they maintained. Unlike most street racers who typically drove recklessly and dangerously, the Midnight Club's priority was the safety of other road users. It may be a strange thing to say considering they go over 300km/h on public highways, but dangerous driving was not allowed. If racers lacked the skill to remain fully in control of the car at high speed or if just once they displayed dangerous driving or careless behaviour, they were kicked out of the club.

In 1999, disaster struck one night. A race broke out between the Midnight Club and the rival Bosozoku biker gang where the race travelled into a high-traffic area, resulting in an enormous crash where two Bosozoku bikers were killed and six innocent civilians were hospitalised. The Midnight Club had failed in their pledge to never bring harm to civilians and overnight the club was disbanded for good. Street racing should not be condoned but Midnight Club did it differently and with style, making their mark in street racing history.

QR codes are essential, but some may hurt you

JINAT JAHAN KHAN

With more dependency on the internet, the cases of online scams are always on the rise. Among different innovative ways to scam people, tricking users through QR codes is a very common scenario. Since the early 2000s, QR codes have been in use, and these are still alive and well. Smartphone cameras can even scan them directly. The continued usefulness of QR codes is due in large part to changes to different marketing channels and new applications for their usage. Popular among modern tech users, QR codes have become essential in transferring large amounts of data by providing an easy and quick way to promote website URLs. However, it pays to be careful when using QR codes.

dangers that are associated with using QR codes.

How can some QR codes be dangerous?

QR codes are inherently not risky. However, these codes may contain phishing or malicious URLs or bugs that involve security threats making these codes dangerous. While it is usually safe to use QR codes, there are certain ways your information could be confiscated by a malicious third party. Here are some ways in which QR codes can cause you notable harm.

Phishing scams through QR codes
QR codes are often used in phishing attacks known as QPhishing. In this method, a cyber criminal replaces a legitimate code with a QR code

steal your confidential information and send them to criminals. Sometimes these malware attacks can be ransomware attacks where cyber criminals hold your data and information hostage for a ransom.

Bugs in QR codes
If there is a bug in a QR code, the bug gets triggered whenever a user points their camera at that code. Hackers may use this bug to exploit the cameras or sensors of users' smartphones and other devices, redirecting them to various malicious and inappropriate websites. These bugs can also manipulate the genuine URLs within QR codes.

Financial theft
Since QR codes are a popular and efficient way to carry out different transactions

Despite the potential of personal and financial damage, there isn't a reason to be scared of QR codes as long as you're careful. Below are some recommendations on being safe while using QR codes.

Use QR codes only from trustworthy sources
To remain careful, it is best to scan QR codes only from reliable sources. It is highly recommended not to scan any random QR codes that are too exposed or can be found in any usual public place. To ensure that a source is trustworthy, check the website URL and security, such as looking for its SSL certificate.

An SSL certificate refers to a digital certificate that helps authenticate a website's identity. Here, SSL or Security Sockets Layer is a security protocol. It keeps internet connections secure, ensuring that criminals are prevented from reading and modifying information. If there is a padlock icon next to the URL in the web address, it means that SSL protects the website and it is safe to visit it. Only after being fully confirmed about security measures and trustworthiness, a person should share information or carry out any transaction.

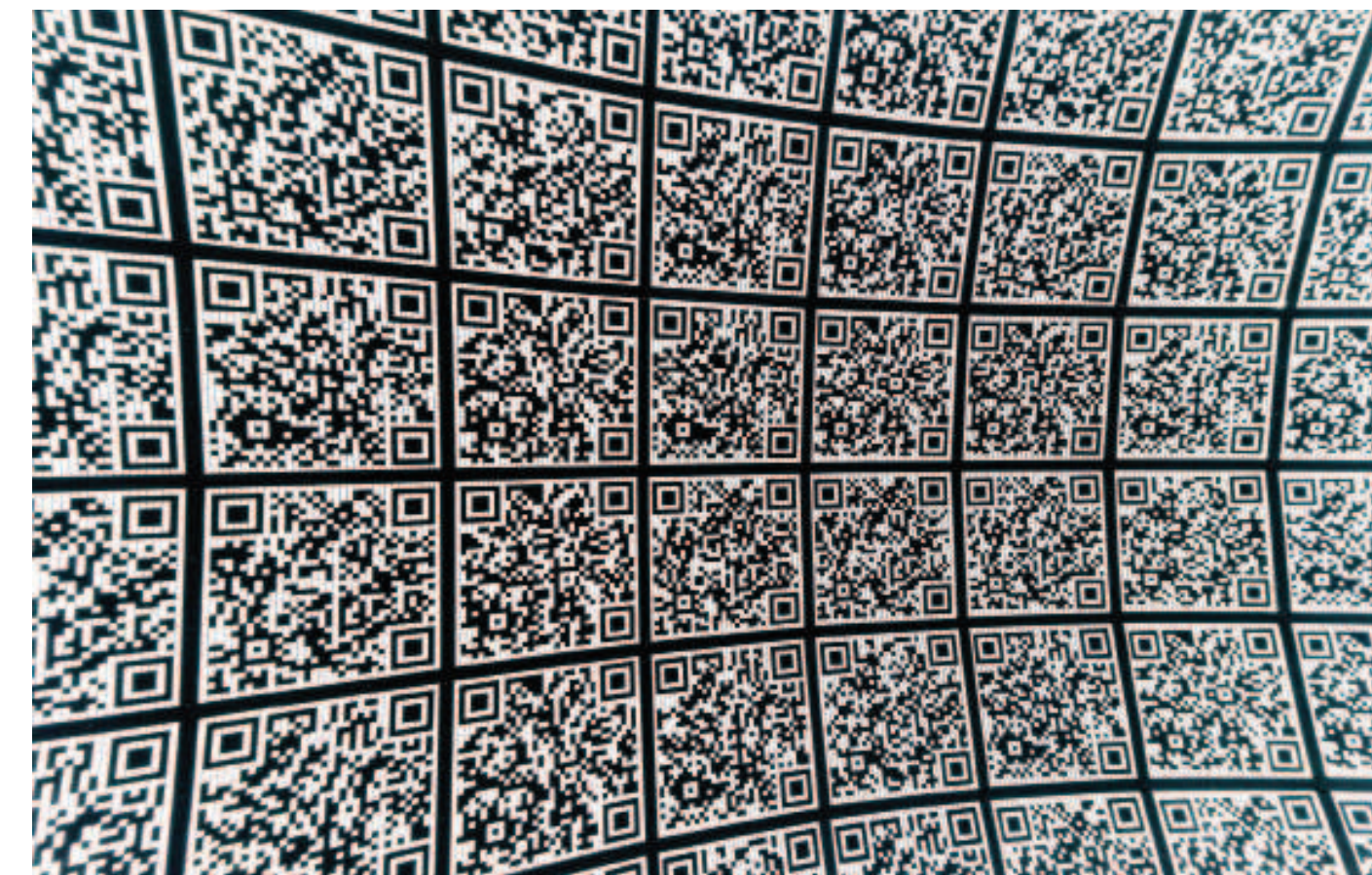*Update the device's security on a regular basis*
Installing and updating your smartphone or any device's security software patches provide security to all your information and data. Moreover, installing some anti-malware software such as Emsisoft Emergency Kit review, Bitdefender Antivirus Free Edition, AVG AntiVirus Free and Avira Free Security Suite may provide an extra layer of security to your devices from malicious activities and can notify you instantly in case any suspicious activity is found.

Use QR scanners to maintain security
Always use QR scanners that display URLs before opening them instantly. Most third-party scanners have a feature in which they directly display the website after scanning the code. It may seem more convenient and efficient, but it can be dangerous in case it contains some malicious factor. Therefore, it is best to use a built-in QR scanner that generally comes with a smartphone camera. It shows the site link before opening it directly. Thus, the user has the option to close the link before it gets opened if something seems dubious.

Be cautious at all times
When you are about to scan a QR code, check if there is any suspicious frame text, or if the displayed logo or the website URL after scanning seems to be different or tampered with. Pay close attention to detail. If anything seems wrong, it is recommended not to use it and find any different mode to share information and transactions.

What are QR codes?

QR codes or 'Quick Response' codes are capable of storing a lot of information and data. They are essentially barcodes that are frequently used to track information about goods and services in a supply chain and in marketing and advertising campaigns.

Interestingly, it does not matter how much information a QR code contains. Once scanned, it will allow the user to access all of its data instantly. Hence, it justifies its name 'Quick Response'. Even if these codes are efficient and easy to use, we should not overlook the risks and

embedded with a phishing website URL, which does not look suspicious at all. Scammers can use catchy lines such as "Scan to win a surprise gift" to exploit your curiosity and steal your information, especially in public places. Such codes can even be deployed in an email to breach your data.

Triggering malware attacks
Cybercriminals may present QR codes embedded with malicious URLs so that whoever scans the code gets infected by the malware. It can harm the users by opening backdoors for more malware attacks or infections, or it can silently

and pay bills instantly. Unfortunately, fraudsters can take advantage of such codes to steal money from people.

The use of QR codes has increased exponentially after the Covid-19 pandemic, to promote contactless communication and information exchange. Now, these are largely used at shops and restaurants to pay bills, show menu cards or discount offers. However, scammers may replace these legitimate codes, especially in public places, with wrong account details to scam unsuspecting passersby.

How to be safe while using QR codes