Check Point Software warns mobile users of QR code scams

As the use of QR codes has exploded during the Covid-19 pandemic, cybersecurity solutions company Check Point Software Technologies is warning mobile users of the security risks that come with it.

Photo by David Dvorácek on Unsplash

Concerns over Covid-19 transmission has seen restaurants adopting QR codes so that customers can browse menus on their phone or make contactless payments, and QR codes recording check-ins at venues via contact tracing apps.

Hackers are looking to take advantage of QR codes' new popularity by replacing legitimate QR codes with one that launches a malicious URL or tries to download customised malware when scanned. Earlier in 2020, Belgian federal police issued a warning about an online fraud involving QR codes.

When scanned, the malicious code tries to access the login credentials used for other apps on a user's phone – such as banking and retail apps – to try to steal login data or set up unauthorised transactions. ING Bank in the Netherlands has also warned of fraudulent QR codes, which attempt to link a second person to customers' ING accounts via the ING bank's phone app.

A recent survey by MobileIron showed that from March to September 2020, 38% of respondents scanned a QR code at a restaurant, bar or café, and 37% scanned a code at a retailer.

Over half (51%) of respondents stated they do not have, or did not know if they had security software installed on their phones. In many cases, these phones hold both personal and business apps and data, putting organisations at increased cyber-risk. Check Point's 2020 Cyber Security Report showed that 27% of organisations worldwide were impacted by cyber-attacks involving mobiles, and 34% hit by mobile malware.

QR codes are not inherently secure or trustworthy

A spokesperson of Check Point Software said the following: "We need to remember that a QR code is nothing more than a quick and convenient way to access an online resource, and we can't be certain that the resource is legitimate until after we've already scanned the code – which means that an attack could have already started."

“QR codes are not inherently secure or trustworthy, and hackers know that a majority of people have little or no security on their phones at all, so we strongly advise everyone to use a mobile security solution to protect their devices and data against phishing, malicious apps and malware.”