CYBER GUIDANCE ISSUE 00038

MALICIOUS QR CODE SECURITY CONCERNS

DATE ISSUED: 21st September 2020

IMPACT	LOW	MEDIUM	HIGH ◄
EASE OF EXPLOIT	LOW ◄	MEDIUM	HIGH
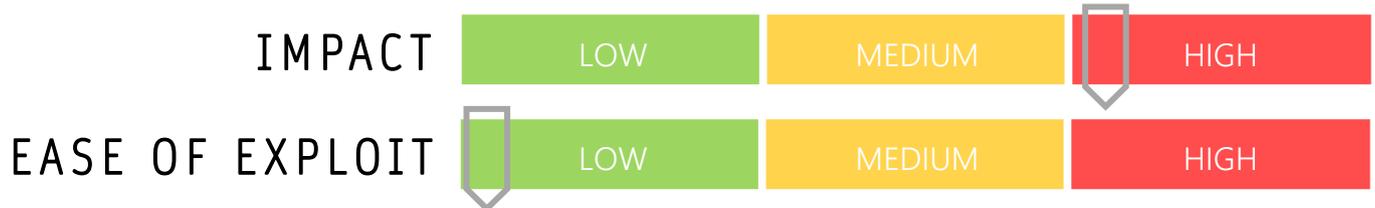
OVERVIEW

The use of QR (Quick Response) codes has been implemented in in many Covid-19 activity tracking applications to allow bricks and mortar businesses to operate without having to manually record everyone who visits their premises. These scannable codes may be used to easily used to curate cyber-attacks.

BREAKDOWN

Also used in place of paper advertising and brochures, QR scanning codes have seen wide adoption for uses in Covid-19 tracing applications. 71% of people surveyed by MobileIron revealed they revealed they have no knowledge in how to discern a legitimate code from a malicious one. By scanning these codes, a user is often directed to a website or some other immediate action such as logging without providing information on the actions performed. Malicious URLs or software can be embedded into a QR code or the user may be pointed to a phishing or spoofed website in place of the legitimate one.

REMEDIATION STEPS

- Ensure all scanning devices that interact with QR codes have anti-malware and/or traffic monitoring software installed and enabled on them to detect malicious software, unauthorised downloads or redirections to malicious sites and prevent further action.
- Be cautious when scanning QR codes from unknown sources
- Check no stickers or covering posters have been placed over the top of the legitimate QR code
- Check URLs that you have been directed to are legitimate and never share personal information on website visited through QR codes that seem suspicious. A good indicator is the padlock present in the search bar of your browser to show the site is encrypted.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/qr-codes-menu-security-concerns/159275/
Infosec Institute: https://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref
Lifewire: https://www.lifewire.com/how-to-protect-yourself-from-malicious-qr-codes-2487772
Sophos: https://news.sophos.com/en-us/2019/10/17/beware-the-square-how-to-spot-malicious-qr-codes/