

QR codes pose internet security risk

February 19 2014, by Candice Barnes



QR code for the Murdoch University website

Internet security experts from Murdoch University have raised concerns about the growing use of Quick Response codes, also known as QR codes.

Dr Nik Thompson said because the codes can only be read by a machine, such as a smart phone, it is difficult for people to determine what they are about to download.

"There have already been cases of QR codes used maliciously to install malware on devices, or direct them to questionable websites," he said.

The codes, which are often used in marketing campaigns, could also be used to subscribe people to unwanted services, such as premium SMS.

In one recent case, a poster with a QR code was placed on the wall at a [security](#) conference, inviting passers-by to scan the code to win an iPad.

During the weekend conference, 445 people scanned this code and visited the linked website.

"The fact that so many people were willing to scan this untrusted QR code, even at a conference dedicated to IT security, highlights the possibly dangerous level of trust that is placed in printed materials such as posters," he said.

"Most of us are familiar with standard barcodes, which have been used safely for decades, and so don't understand the risks associated with QR codes."

A standard barcode can represent up to 20 characters of information, while QR codes can carry much more data – up to thousands to characters.

Originally used in the automotive industry, QR codes are now used to direct people to URLs, contact details and other online content.

To avoid the scammers, Dr Thompson suggests using QR code readers which allow you to preview the entire URL before proceeding to the site.

He also recommends seeking out one of the many anti-malware apps available, developed by well-known internet security companies.

"Internet users need to be just as cautious with their mobile and tablet devices as they are with their laptop and desktop computers," Dr Thompson said.

"Never log in or submit personal details to any website you access by QR code, as it could be a fake site set up to capture your information.

"Criminals follow the money, so if more people are using mobile devices, that's what they're going to target."

Provided by Murdoch University

Citation: QR codes pose internet security risk (2014, February 19) retrieved 28 April 2024 from <https://phys.org/news/2014-02-qr-codes-pose-internet.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.