A rapidly growing social interaction technology is the use of Quick Response (QR) codes as physical shortcuts to Internet resources. QR codes are matrix barcodes that are traditionally used to identify automotive components. QR codes are touted for their ease of use and convenience and are increasingly being used for marketing and social interaction. This is commonly done by placing a QR code on an automobile component or poster, which, when scanned by a person with their mobile phone, directs them to a website.

QR codes implemented in this way often provide little more than a physical, machine-recognizable representation of a hyperlink, appearing on posters, newspapers and even television. An individual uses their mobile phone camera to quickly capture the QR code which then directs them to a website. The user is presented with product information and often asked for personal information. Marketers love QR codes as they allow them to target their chosen groups of users and specific locations, but these properties are also the reasons why QR codes could be the next phishing risk.

Any individual or company can create QR codes by using simple web-based generators that encode URLs as their own unique QR representation. In fact, certain popular website redirection services now generate a QR code for every website simply as a matter of course. QR codes typically hold around 50 characters, with newer more compact versions holding up to 1284 alpha-numeric characters. This space is sufficient to allow the encoding of information such as the QR location (e.g. poster location), descriptive meta-data as well as a destination website.

**Cause for concern**

There are a number of reasons why the public should be concerned about the widespread use of QR codes. Phishing is the activity of attempting to gain personal information from a user by masquerading as a legitimate site or organisation. The term phishing was coined by attackers who are ‘phishing’ for information. This information may be bank or credit card details, or even other personally identifying information such as mother’s maiden name and postal addresses to be used in subsequent identity theft. One of the key elements to misleading the user to a malicious site is to obfuscate the URL and prevent them from identifying the malicious site until it’s too late. QR codes, as they are not human-readable, are the ultimate form of URL obfuscation service. However, because of the unique way in which users access QR codes, there may be a perception they are safer than links in phishing emails, for example.

Many tricks have been used in phishing emails; these include cloning the website of a reputable company, obscuring the actual destination address of a link and using redirection services to mislead the user as to what exactly they are clicking on. However, as is to be expected, users are more careful than they once were and would-be attackers need to resort to new means to get their victims to click on an untrusted link. The fact that QR codes are often physical objects such as posters may increase the users’ perception of safety as they may feel that they are interacting with a real, tangible thing rather than an untrusted website link. If part of the solution for a security weakness relies on the user to make a decision, then simply changing the context of the situation may lead the user to make a different (and thus insecure) choice.

**Same tricks**

As it happens, the QR code in its current implementation actually deploys many of the very techniques that phishing scammers use to mislead their victims. In the quest for convenience and ease of use, developers have overlooked many of the lessons learned from the past. Add to this the fundamental misunderstanding that the smartphone is any different or safer than any home PC, and there is a recipe for disaster.

Aside from email filters and antivirus warnings, the bottom line for defence against malicious websites is the user. The user needs to evaluate the situation and make a decision not to click on something that they are not entirely sure about. QR code readers commonly installed with smartphones trivialise, or sometimes even omit, this decision altogether. Some QR readers only display part of the destination website whereas certain QR readers do not even prompt the user for confirmation before accessing the destination website. This program behaviour removes the user’s ability to check the location of the website they are visiting.

Another commonly used phishing technique is to convince the user to visit a seemingly innocuous website, and then redirect them elsewhere automatically. This approach, using URL redirection services, is relatively simple to implement and many QR codes are embedded with a shortened URL that gives the user absolutely no information for them to differentiate one destination website from another. Services such as bit.ly and tinyurl.com are promoted as URL shortening services, and produce URLS that are indistinguishable from one another at a glance (e.g. bit.ly/sdfds vs. bit.ly/fdsfa). This technique is breaking the ‘read first, click later’ behaviour that is desired amongst users.

**Popularity means greater target**

Targeted phishing attacks are gaining in popularity, as the success rate of the attack is dramatically improved with careful selection of the target. By virtue of self-selection, QR code scanning attacks are often targeted. For example, a QR code on a property listing would be an ideal placement for a real estate scam. This QR code would be scanned only by those interested in real estate, thus saving the attacker the effort of selecting potential victims. Furthermore, as the user is the one who initiates the request, it is possible that they may inherently also place more trust in the website they are accessing.

To add to the threat, accessing websites from QR codes can reveal a wealth of rich information to the phisher. Simply visiting a website generates a wealth of rich metadata such as device location, device connectivity history, device version and more. By visiting the website, they may feel that they are interacting with a real, tangible thing rather than an untrusted website link. These properties are also the reasons why QR codes are promoted as URL shortening services, and produce URLs that are indistinguishable from other links in phishing emails.

As new technologies emerge, they bring with them new risks to users’ privacy and security. Technical security vulnerabilities are often attuned. However, research suggests that human factors are potentially the biggest weakness in an otherwise well-secured system. Users are persuaded. However, research suggests that human factors are potentially the biggest weakness in an otherwise well-secured system. Users are persuaded.

By Nik Thompson and Kevin Lee

Are QR Codes the Next Phishing Risk? Their ease of use could be making Quick Response codes a security threat.

Nik Thompson and Kevin Lee are lecturers at the School of Information Technology at Murdoch University and both ACS Certified Professionals (CR). They are currently undertaking a project to examine the security of personal information in the context of the rapid uptake of new communication and interaction technology.