Malicious QR Codes: Unexpected and Unwanted

Keirsten Henson, Appalachian State University, USA
Beverly Medlin, Appalachian State University, USA
Sandra Vannoy, Appalachian State University, USA

Abstract

Recently, QR codes (Quick Response Codes) have become popular due to their inexpensive costs and ease in creating unique and scannable barcodes that can direct smartphone users to certain websites or other downloadable content. Unfortunately, criminals are taking advantage of QR codes by getting victims to access a possible page that may contain malicious activities. Though QR codes have several advantages, there are issues related to security that have been fairly overlooked. As QR codes become more prevalent with mobile shopping on the rise, and all you need is a mobile phone with a camera, and a mobile app that can scan, store, and share QR codes, this activity is very simple. But this simplistic action by the end user and retailer is also simple for a hacker. As the mobile market outpaces PC sales, newer, mostly end-user devices such as smartphones are the least likely to include any type of security software. This paper addresses the background of QR codes and next to the security concerns that may be unexpected and certainly unwanted.

Introduction

The symbol known as a Quick Response (QR) code is a two dimensional (matrix) that was introduced in 1994, initially as a means to track parts used in automobile manufacturing in Denso Wave - one of Japan's Toyota group of companies (Brindha and Gopikaarani, 2014). The patent was made available for public use and as an international standard that was approved by the International Standards organization in 2000 (ISO, 2015).

Similar to the use of QR codes in the automobile industry, QR codes can be used in a number of areas as a means or method to support interaction in controlled situations such as in education. Examples include marking assessment (Bhaturkar and Bagde, 2014), providing formative feedback in class (Susono and Shimomura, 2006), and protecting the integrity of online examinations (Soman et al., 2013). In the scenarios above, the QR code is created by the "controlling" central party (e.g., the professor) and distributed too many client users (students), either the same to all, or personalized for a group of students or one individual student.

It was the emergence of the smartphone, however, that relegated QR technology to the mainstream, giving organizations the means by which to direct traffic to their products and services and provide novel means of payment (Kharraz et al, 2014). QR codes are now being used extensively across a number of fields and applications. For marketers, QR codes have allowed advertisers to engage in promotions such as event advertisements, brochures, and posters. Additionally, clothing and billboards have been used to direct users to mobile pages that can contain much more information and interactivity than can be afforded on the printed page. This integration between print and web via mobile devices adds a new dimension of communication to any marketing or outreach effort or campaign. In Chennai, India QR codes are even being used to make sure that public toilets are clean. Eram Scientific has created a new form of e-toilet QR code that allows the user to scan a barcode with their smartphone so they can provide remarks and suggestions. Upon scanning the code with their smartphone, the end user is directed to a feedback portal where they can leave messages about the cleanliness and maintenance of the public restroom system in over 210 locations (E-toilet QR codes help to improve public bathroom cleanliness and maintenance, 2017).

A more recent purpose for QR codes is that of handling payments. A seller creates a QR code that corresponds to a good or service. Upon scanning the code, the user is directed to an intermediate or company-managed payment system where the user can either store or enter in the bank, debit card, or credit card information. While this process is very convenient for the company and the end consumer, it also brings a number of risks that will be discussed later in this paper (Krömer et al., 2017).

This paper addresses the malicious activities of QR usage as most research noted previously has only identified its advantages or benefits. In addition, recommendations are offered to end users in regard to security and QR scanning.

There are a number of commercial as well as free applications tools that can be used to generate a QR code (Wainwright, 2015), as noted in Tables 1 and 2. After creation of the code there must be a means to decode it and obtain the content – either by software that is pre-installed on the client device (e. g., a suitable mobile application), and/or by accessing a remote server to obtain the content or the parts of it that may be required for user authentication.

Literature Review

QR codes have two major functions (Rouillard, 2008). First, due to the high data-density of the encoding (approximately 100 times more than a bar code) a QR code can contain significantly more information than a bar code while occupying a comparable space slot (up to 7000 alphanumeric characters), and secondly, it is able to support encoding of characters such as the ones used in logographic and phonemic writing systems (e. g., Kanji and Kana).

QR codes can be created quickly and easily and often at no cost. If an individual does a search on the Internet for a QR code generator or creator, hundreds of links are found that offer free and paid applications. The applications are generally simple to use as they allow the end user to easily make selections related to QR code creation. The creator can select where the QR takes the reader, such as a URL, phone number, SMS, text, or maps. As noted below in Tables 1 and 2, a sampling of some of the most popular and highly used free QR applications as well as paid QR generators are presented as well as a sampling of their capabilities. Differences between QR Code generators are generally found in the three areas that are listed below.

- The possibility to track and change QR Codes destination
- Quality and resolution of the QR Codes (for posters it may be better to use vector image)
- Customizations with colors, shapes and logo

Of course QR generator offers some of the capabilities listed above, but you will see that whether free or paid they can offer other unique possibilities.

Table 1: Free QR Code Generators

Name	Capabilities
ForQRCode.com	QR codes can be made with different qualities such as PNG, SVG, EPS. The application also supports link locations, email, text, SMS, and call links. Payments can also be made to PayPal.
qr-code-generator.com	Codes are easy and fast to create with different colors and designs. Available QR Code types include a vCard to an Email QR Code. Their codes can also be included in websites.
QRStuff.com	QRStuff offers 100% ad-free codes that are permanent and therefore do not have an expiration date that even some paid QR generators do not offer. They allow the QR creator to generate as many free and permanent codes as that would like. Users can access and use many different file and image types that will not expire. In addition they can create links to sites like YouTube and Google Maps.

Table 2: Paid QR Code Generators

Name	Capabilities	Monthly Cost for Basic Service
Scanova	This application offers links that are for both commercial and personal use. Their products include image, audio, mapping, video and coupon offers among others.	$9.00
Unitag	Unitag offers Advanced scans analytics, dynamic QR redirects and editing as well as colorful codes with capabilities to conduct many market analysis. The codes are presented in high-resolution.	$11.00
Kaywa	Kaywa offers business and personal solutions that can track and analyze usage of the QR code, offers different colors, shapes and logos, as well as custom URLs that offers the unique feature of multiple URLs that can be linked to one QR code.	$13.75

Within the current environment, QR codes may be seen as advantageous, but they can be malicious as well. Actions related to hacking and identify theft, are the nemesis of QR codes and can be a means to capture information and to introduce end users to dangerous and malicious software among other types of destructive attacks. End users, therefore can benefit from QR codes, but can just as easily be a recipient of a malicious attack.

Little research has been conducted concerning the malicious activities of QR codes (Krombholz, 2014). However, because of the growth in popularity among the public and the increasing fraudulent activity regarding QR Codes, more attention needs to be paid to this topic. Popular methods of fraudulent activity include phishing, typosquatting, malware distribution, and browser exploitation among others.

Attributes that may be set within the code include *the size of the QR code, such as S*: One square inch (a perfect size for your business card), and as well as its color. As an example, the QR code below was created using QRStuff.com, a free tool that links you to the website of Appalachian State University.

Figure 1: QR code to Appalachian State University

Creation techniques of QR codes are continually being developed with new inclusions of symbols and different shapes, but issues have arisen such as errors around the decoding process. But there have been successes as well. A novel image blending method of improving the QR code visual significance for marketing purposes is proposed by Baharav and Kakarala (2013); it improves QR code aesthetics and visual significance by embedding images such as brand logos in full color and without negatively impacting the error correction. Furthermore, (Lin et al., 2013a) proposed a systematic QR code beautification framework that allows an individual user to personalize the QR code they create (for example a QR code containing contact details meant to be to be printed on a business card) by selecting visually meaningful patterns.

Despite the promising opportunities QR code use by individuals is not widely spread worldwide (Sasaki et al., 2007, Rouillard, 2008). But the countries of Japan and Korea have heavily adopted the application and use of QR codes in many industries (Ryu and Murdock, 2013, Sago, 2011). More specifically Sago

(2011) found that the participants in their research (college students) did not fully understand how QR codes worked and were not sure whether their mobile phones could read them; therefore, they were not interested in reading a QR code when seeing one. However, participants who showed interest in QR codes were highly likely to use them in the future. Similar results were obtained in more recent work (Ozkaya et al., 2015, Lo, 2014) which also found that even individuals who considered themselves innovative were very likely to use QR codes.

The findings in these studies and also in Okazaki et al. (2012) and Jung et al. (2012) indicated that the perceived usefulness and ease of use of QR codes as well as perceived attractiveness may influence positively user attitudes towards QR codes; a relationship between the type of product being marketed and expected QR use was identified by Narang et al. (2012).

Addressing in part the noticeable lack of increase in customer adoption of QR use, current advances in QR development has focused on improving their appeal. A novel image blending method of improving the QR code visual significance for marketing purposes is proposed by Baharav and Kakarala (2013); it improves QR code aesthetics and visual significance by embedding images such as brand logos in full color, without negatively impacting the error correction. Furthermore (Lin et al., 2013a) propose a systematic QR code beautification framework that allows an individual user to personalize the QR code they create (for example a QR code containing contact details meant to be to be printed on a business card) by selecting visually meaningful patterns.

There are a number of other use contexts that involve creating as well using QR codes by individuals as a tool to transfer information as described by Narayanan (2012). Examples include encoding personal details in a QR code for others to scan and decode on their devices or scanning someone's QR code to load their details onto the reader's phone (i.e., using the QR code as a machine readable personal card), sending and receiving invitations (i.e., encoding detail about an event including location in a QR code which can be posted on Web pages, or printed in other media, to be scanned by people who want to obtain the invitation). Again, all of these activities are advantageous as they allow the sharing of information to happen almost instantaneously and are imagined by most individuals to be occurring in a safe environment. But there are significant security risks that can occur.

While QR codes have provided a user-friendly way for companies to lead people to their websites, provide new forms of marketing, offer payment processes, and direct people to their products and services, improving security is a vital issue that technological innovation must resolve. Efforts are underway to address the security holes around QR codes and provide the authentication technology necessary. QuickOne, has introduced its "QO" technology that provides an authentication code for enterprises and organizations by applying a unique information identification technique to the QR Code. QO promises to provide a means of secure information storage using the Blockchain, as well as a fast and secure payment gateway (QuickOne Launches ICO, 2017). While QO appears promising in providing much-needed security around QR code technology, its effectiveness remains to be seen.

QR Code Security Risks

With mobile phone usage surpassing 2 billion in 2016, the potential security risks associated with QR codes is certainly concerning. Less than 14% of smartphone owners use antivirus software, and approximately 34% use no type of security at all on their devices. Furthermore, even those users with antivirus software installed are afforded little protection, as mobile antivirus software hasn't reached a level of sophistication needed to thwart today's complex and fast-evolving malicious code. Additionally, most mobile apps have no type of security built in, further exacerbating vulnerabilities to attacks such as phishing and malicious software distribution (Rak et al, 2017). With its release of the Apple iOS 11 in September 2017, Apple added QR scanning functionality, enabled by the camera app. Users simply launch the camera app and point their device at a QR code. There is concern that in spite of some warnings, many actions are performed immediately after the initial tap on the QR code notification, and the ease with which QR code scanning can occur will lead the user to scan codes at will, ignoring warning signs and signals (Threat Intelligence Report: QR Code Threat Landscape, 2017).

In 2014, Kharraz et al examined 14 million web pages to determine the prevalence of malicious activity around QR codes. Even four years ago, while their study did not identify wide-scale abuses, these findings did verify the presence of two primary types of attacks: phishing attacks leading end-users to share private and financial information and malicious software distribution that allows the attacker to download private information from the user's device.

QR codes as a mobile payment solution is a relatively new phenomenon. While this service provides convenience to the consumer, it brings serious risks to the end user, such as loss of private information through a phishing attack mechanism. QR code payments fail to capture the same security mechanisms as card-based transactions. With a card, a PIN (personal identification number) is entered into a merchant's device to initiate the transaction, and the card chip must be inserted or the magnetic strip swiped for the transaction to be completed. However, QR codes no PIN or card characteristics read through a machine. The customer's only recourse is to check the authenticity of the transaction by previewing the details of the merchant.

For example, the creator of the malicious QR code redirects the user to a fake site where the user will be misled to enter in credit card or bank information. Other risks are the typical risks associated with visiting untrusted sites, include the installation of malware and spyware on end users' devices and systems (Krömer et al, 2017). This practice is particularly problematic in China. QR Code Press reports that a massive QR code con is underway in China, scamming bicycle renters out of their money across a number of cities in the country. The fraud is carried about by the placement of a fake QR code over the legitimate code. Then renters' payments are directed to the scammer's bank account rather than the legitimate bike rental company (QR code con culprits identified in China, 2017). Malicious QR code usage has become so rampant in China that the People's Bank of China has prohibited their use as a vehicle for mobile payments.

The QR code payment platform is highly unregulated, meaning it allows transactions without the protection of traditionally regulated financial systems. This allows unqualified merchants to able to operate due to low security thresholds. It also allows fraudulent transactions, fake identities, and stolen funds by allowing transactions that do not comply with financial industry security standards (Hidden risks with 2D QR code payment, 2014).

The ease of use and creation of QR codes have found new adopters. New adopters, and all users may not be aware that cyber criminals use these same applications to introduce malicious QR codes.

The ease with which one can create and distribute QR codes has not only attracted businesses, but the criminal element as well. QR Codes, like many other mobile applications, have been developed with little forethought to security. While most of us will think twice about opening a questionable email or visiting an uncertain website, we often have no qualms about scanning a QR code. Most people are unaware that scanning an unknown QR code offers serious security concerns. While the QR code itself isn't dangerous, there is no opportunity to evaluate the site it will lead you to such as the case with an email or website. If the barcode application displays the URL, an observant user may notice a suspicious-looking URL. However, URL shorteners can make it more difficult for users to evaluate the legitimacy of a URL (Vidas et al., 2012). Typically, the end user reads the code without evaluating risks, and then suffers the consequences if there are security problems.

It is quite easy for a sticker to be printed containing a malicious QR code and then attached over the legitimate code, a type of attack that is known as attagging. QR codes are the perfect vehicle for malicious attacks, facilitating phishing (QRishing) attacks and redirecting users to malicious websites that host viruses, worms, and Trojans (Jain and Shanbhag, 2012). Malicious embedded URLs can lead to malware being installed on mobile devices and result in the loss of sensitive personal data and even damage to software and hardware (Narayanan, 2012).

When a user takes a photo of a QR code, the link it stores is first displayed on the device's screen; however, cybercriminals also use URL shortening services (such as bit.ly and others) to disguise the

ultimate address stored in the QR code which may lead to a page with malware that steals the user's credentials or to a phishing site (Malenkovich, 2015).

QR codes are seen in magazines, on billboards, and on storefronts. They seem to be anywhere and everywhere. Because of the unique ability of QR codes to bridge the gap between virtual reality and actual reality, many consumers forget that QR codes pose the same dangers as emails and websites that can have the ability to capture personal information and to use that information in a fraudulent manner.

The general design of QR codes makes it impossible to distinguish one from another with the human eye, meaning that anyone can replace legitimate codes with an illegitimate one using a sheet of QR coded stickers. In Russia, cybercriminals used imposter QR codes to siphon cash and personal information from hundreds of smartphone owners in 2011 and were refining their methods to dupe even more users.

As previously mentioned, a QR code is a square matrix consisting of either a small black or colored arrangement of dots that can be used to direct end users to a location, event, or other information. Hacking a QR code is not possible as it means manipulation of the action of the code without modifying the code, and this action is not possible. Thus, codes cannot be hacked, but they can be malicious and can trigger malicious activities or actions. But the newly created QR code will not be the same as the legitimate QR code as each contains different patterns. Even though the patterns may be different it is difficult to often dictate a change in the appearance of the code or have knowledge that the code has been manipulated. Noted below are some of the most malicious and popular types of manipulating QR codes.

Typosquatting is the intentional registration of misspellings of popular website addresses (Krombholz, 2014). It is also another type of phishing used to attack QR codes. In 2010 it was estimated that 938,000 typosquatting domains targeted the top 3,264 sites with the domain name ".com" (Moore and Edelman, 2010). This proves that typosquatting and phishing tactics are widely used and effective methods of security breaches.

Currently, mostly Android cellphone users are targeted through a method of download attacks known as "drive bys." These attacks distribute malware by forcefully downloading software onto their device upon visiting a website. These attacks can leak personal data and send SMS to premium numbers (Shankdhar, 2015).

Browser exploitation is another method of popular fraudulent activity related to QR codes. This type of attack can do significant harm to personal devices and personal information. Browser exploitation can send emails, access browser history, and enable camera and microphone capabilities. These actions occur in the background, so users never know about this (Shankdhar, 2015).

One of the growing risks associated with the use of QR codes is ransomware, a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid (Fruhlinger, 2017). The end user scans a malicious QR code and is directed to a site demanding payment in exchange for the release of their private files and information. Interestingly, one of the most devastating ransomware platforms, Rokku, actually provides a QR code to the victim, leading them to a payment platform for making the ransom payment (Bisson, 2016).

After addressing some of the dangers of QR codes, a combination of the above-stated danger factors do not incentivize or do much to spur consumer confidence in the technology—or enhance its adoption rate.

PREVENTATIVE END USER ACTIONS

Fortunately, there are preemptive solutions to the malicious activity surrounding QR codes. By using these defensive tactics, users can simply refuse the unpredictability of corrupt QR codes. ☐ Observe closely before use. If possible, touch the QR code and ensure there is not a fake code stuck on top of the real code.

- Never provide personal data. Real QR codes will never request personal information.
- Identify URL before use. To ensure a secure connection, look for "https" in the URL (Kaur, 2017).

- Download Norton Snap. This is a QR code scanner application available on both iOS and Android devices with built-in security features. This application checks for malicious patterns within the QR code (Krombholz, 2014).
- Security Awareness Training. End users of QR codes must be purposeful about being sensitized to the associated risks.
- Securing smartphones. End users of QR codes can significantly reduce the negative effects of malicious QR code by following simple security guidelines, such as installing antivirus software and thinking before downloading questionable apps.

As noted previously, end users must become vigilant in their security concerns as their adoption of QR code use rises on their mobile devices and in public spaces. Commercial use of QR codes are on the rise.

Conclusions

The general design of a QR code makes it easy and cheap to create, as well as impossible to identify as a "good" QR code versus a "harmful" one. But there are steps that companies and individuals must assume before simply scanning a random QR code and trusting that it will not introduce malicious code or do harm rather than good. Simply put, end users should never trust any QR code and be suspicious and alert to where any QR code may take them.

Unfortunately, for smartphone users, there are multitudes of QR readers in every app store, and all of them offer a slightly different user experience. None of the big three (iOS, Android, or WP7) offer a native application, and therefore there is no dominant brand of reader. So users simply must select QR readers essentially at random, and hope for the best.

Lastly, end users must ask themselves "Is it worth clicking on a QR code symbol worth the harmful consequences," that might be caused?

References

Baharav, Z. & Kakarala, A, R. 2013. Visually significant QR codes: Image blending and statistical analysis. Multimedia and Expo (ICME), 2013 IEEE International Conference, 1-6.

Borrett, L. 2011. Beware of Malicious QR codes. Retrieved from http://www.abc.net.au/news/technology/ on April 7, 2016.

Bhaturkar, K. P. & Bagde, K. G. 2014. QR code based digitized marksheet. International Journal of Management, IT and Engineering, 4, 57.

Bisson, D. "Trouble paying the ransom? This ransomware provides QR code for mobile payment." Retrieved from https://www.grahamcluley.com/rokku-ransomware-code/ January 11, 2018.

Brindha, G. & Gopikaarani, N, 2014. Secure banking using QR code. International Journal of Advanced Research in Computer Engineering & Technology. 3(12), 4302-4306.

"E-toilet QR codes help to improve public bathroom cleanliness and maintenance." Retrieved from http://www.qrcodepress.com/e-toilet-qr-codes-help-improve-public-bathroom-cleanlinessmaintenance/8533658/ on January 11, 2018.

Fruhlinger, J. "What is ransomware? How it works and how to remove it." Retrieved from https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-worksand-how-to-remove-it.html on January 11, 2018.

"Hidden risks with 2D QR code payment." Retrieved from https://www.linkedin.com/pulse/20140907174521-104874410-hidden-risks-with-2d-qr-codepayment/ on January 11, 2017.

ISO.2015. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=43655, March 1, 2016. Jain, A. K., & Shanbhag, D., 2012. Addressing security and privacy risks in mobile applications. IT Professional, (5), 28-33.

Jung, J.-H., Somerstein, R. & Kwon, E. S., 2012. Should i scan or should i go?: Young consumers'motivations for scanning qr code advertising. International Journal of Mobile Marketing, 7.

Kaur, S. 2017. QR Code Security and Solution. International Journal of Engineering Science and Computing, 7(4), 10323-10225.

Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., & Francillon, A. (2014, June). Optical delusions: A study of malicious QR codes in the wild. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on (pp. 192-203). IEEE.

Krombholz, K., Fruhwirt, P., Kieseberg, P., Kapsalis, I., Huber, M. & Weippl, E. 2014. QR Code Security: A Survey of Attacks and Challenges for Usable Security. International Conference on Human Aspects of Information Security, Privacy, and Trust, 79-90.

Krömer, P., Alba, E., Pan, J. S., & Snášel, V. (Eds.). (2017). Proceedings of the Fourth Euro-China Conference on Intelligent Data Analysis and Applications (Vol. 682). Springer.

Lin, Y.-H., Chang, Y.-P. & Wu, J.-L., 2013a. Appearance-based QR code beautifier. Multimedia, IEEE Transactions, 15, 2198-2207.

Lo, H., 2014. Quick response codes around us: Personality traits, attitudes toward innovation, and acceptance. Journal of Electronic Commerce Research, 15, 35-39.

Malenkovich, 2015. Retrieved from https://blog.kaspersky.com/qr-codes-convenient-dangerous/1115/ on April 8, 2015.

Moore, R., Lopes, J., 1999. Paper templates. In TEMPLATE'06, 1st International Conference on Template Production. SCITEPRESS.

Moore, T. & Edelman, B. 2010. Measuring the Perpetrators and Funders of Typosquatting. Financial Cryptography and Data Security: Proceedings of the International Conference, 1-5.

Narang, S., Jain, V. & Roy, S. 2012. Effect of QR codes on consumer attitudes. International Journal of Mobile Marketing, 7, 52-64.

Narayanan, S. (2012), QR Codes and Security Solutions. International Journal of Computer Science and Telecommunications, 3(7), 69-72. Okazaki, S., Li, H. & Hirose, M., 2012. Benchmarking the use of QR code in mobile promotion. Journal of Advertising Research, 52, 102-117.

Ozkaya, E., Ozkaya, H. E., Roxas, J., Bryant, F. & Whitson, D., 2015. Factors affecting consumer usage of QR codes. Journal of Direct, Data and Digital Marketing Practice, 16, 209-224.

"QuickOne Launches ICO." Retrieved from http://bitcoinist.com/quick-one-launches-ico-based-on-newlydeveloped-qr-code-technology-that-may-become-the-future-of-ultra-secure-information-sharingidentification-easy-online-payments/ on January 11, 2018.

"QR code con culprits identified in China." Retrieved from http://www.qrcodepress.com/qr-code-conculprits-identified-china/8533207/ on January 11, 2018.

Rak, J., Bay, J., Kotenko, I., Popyack, L., Skormin, V., & Szczypiorski, K. (Eds.). (2017). Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings (Vol. 10446). Springer.

Rouillard, J., 2008. Contextual QR Codes. Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology (ICCGI 2008). IEEE.

Ryu, J. S. & Murdock, K. 2013., Consumer acceptance of mobile marketing communications using the QR code. Journal of Direct, Data and Digital Marketing Practice, 15, 111-124.

Sago, B., 2011. The usage level and Effectiveness of Quick Response (QR) codes for integrated marketing communication purposes among college students. International Journal of Integrated Marketing Communications, 3, 7-17.

Sasaki, J., Shimomukai, H., Yoneda, T. & Funyu, Y., 2007. Development of Designed QR Code. Frontiers in Artificial Intelligence and Applications, 154, 290.

"Scanning QR Codes: Be Safe." Retrieved from http://beqrioustracker.com/scanning-qr-codes-be-safe/ on April 8, 2016.

Shankdhar, P. 2015. Security Attacks via Malicious QR Codes. Retrieved from http://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref.

Soman, N., Shelke, U. & Patel, S., 2013. Automated Examination Using QR Code. International Journal of Engineering and Advanced Technology, 2, 622-627.

Susono, H. & Shimomura, T., 2006. Using mobile phones and QR codes for formative class assessment. Current developments in technology-assisted education, 2, 1006-1010.

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L, 2012. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. CyLab: Carnegie Mellon University, 12 pgs. Wainwright, C., 2015. How to make a QR code in 4 quick steps [Online]. Available: http://blog.hubspot.com/blog/tabid/6307/bid/29449/How-to-Create-a-QR-Code-in-4-QuickSteps.aspx [Accessed 1 March 2016]. Zhou, Y. & Jiang, X., 2012. "Dissecting Android Malware: Characterization and Evolution," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, pp. 95-109.