International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 9, September - 2022, Pages: 10-15

Confidentiality of Information when Using QR-Coding

Zhanna Deineko[1], Svitlana Sotnik[2], Vyacheslav Lyashenko[1]

[1]Department of Media Systems and Technology, Kharkiv National University of Radio Electronics, Ukraine
e-mail: lyashenko.vyacheslav@gmail.com

[2]Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv National University of Radio Electronics, Ukraine

Abstract: *This work is overview in field of QR codes and their application. The main attention is paid to confidentiality of personal data both when using QR codes and when creating them. The key rules for coding are given. The paper contains main recommendations in order to prevent involuntary transfer of their personal data. Also identified are key aspects that you need to pay attention to in order to make sure that QR-code is secure.*

Keywords—review; information coding; QR code; privacy; security; phishing

1. INTRODUCTION

QR codes are modern breakthrough in field of digitalization, because encoding of information is carried out in order to simplify its further extraction by automated means.

In today's world, information can be presented in different forms. The encoded information can be text, phone number, or even website URL.

The surge of QR codes is caused by fact that it is enough to have phone with you, with which you can scan code and quickly get necessary information.

QR codes can not only be conduits to information world, but also used to organize checkpoint.

QR codes of data or information can track number of scans, location of scan, device used in scan, and date of scan.

Although theoretically and in practice QR codes are protected, however, people do not always handle codes correctly – this can cause phishing risks, that is, obtaining unauthorized access to confidential information (such as usernames, passwords, credit card information, and network credentials).

With modern integration of QR code technology into all aspects of our online lives, QR codes are also used in phishing [1]-[3]. At the same time, we can use various methods and approaches to create and decrypt QR codes [4]-[15]. Thus, issue of information confidentiality in QR code is becoming more relevant every day.

2. RELATED WORK

A number of works are devoted to ensuring security when using QR technologies.

In [3], authors offer secure authentication system using secret key and QR codes. The developed authentication system is applicable to special mobile application for authentication, which will eliminate process of entering website credentials and, as result, will provide reliability for phishing.

QR-coding systems today are used as effective methods: information transfer [16]; information protection, for example in medicine [17]; implementation of any scale payments [18], to which significant number of works are devoted.

In [16], authors use both QR code and blockchain functions for transparent, distributed, and reliable inventory management. A secure QR code-based messaging system speeds up inventory management.

In [17] authors investigate ECG steganography using discrete wavelet transform (DWT) and rapid response code (QR). The QR code is embedded in 2D image using an additive quantization scheme. QR code provides reliable protection of patient data with full retrieval capability.

In [18] authors describe use of mobile payment system based on QR code. Transaction data generated using QR code.

The use and prospects for use of QR codes were previously considered by us in [19].

The security of private information is described in [20]. The authors offer dual modulated QR codes (DMQR) with which users can securely transmit personal information in public places using their smartphones and camera interface.

In [21] proposes algorithm for hiding confidential information by changing QR code modules. The authors also offered additional feature in their work – authorized users with secret key can additionally extract hidden confidential information

In [22] presents study of 2D barcode threats and available protection mechanisms. The authors offered guidance on how to use barcode for recommended image and data sizes at different levels of use. A comparison of digital signature and encryption mechanisms based on usability and security is provided.

In [23] analyzed security and privacy of 100 barcode scanner applications. The authors cited set of guidelines that developers should follow to create convenient, secure, and privacy-friendly barcode scanning apps.

International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 9, September - 2022, Pages: 10-15

3. ENCODING TYPES

There are two basic types of coding:

- one-dimensional;

- two-dimensional.

Today there are more than 50 types of one-dimensional barcodes, they are also called 1D [24], [25].

The one-dimensional code is presented as combination of vertical stripes of black and white of different widths with combination of numbers under them.

Recognition of one-dimensional barcodes is fast and with fewer errors.

A feature of 1D barcode is for encoding small amount of information about product or service.

Disadvantages of one-dimensional coding:

- as a rule, cheap in development and printing (compared to two-dimensional);

- recognition of one-dimensional codes is fast and with fewer errors.

Advantages of one-dimensional coding:

- stores relatively small amount of information (contains up to 30 characters of information);

- stores numerical data and cannot easily create unique codes;

- if code is damaged, probability of reading is reduced;

- read from short distance;

- time of their scanning takes more time than their "insertion into products";

- codes are easily susceptible to forgery.

There are 70 types of two-dimensional barcodes called 2D.

Two-dimensional code is represented a combination of graphical objects, which are two-dimensional matrix of black and white dots or modules.

The peculiarity is that in code, unlike one-dimensional coding, two-dimensional 2D scanner perceives code as whole as image, and recognizes it in aggregate.

Disadvantages of two-dimensional coding:

- stores large amounts of information;

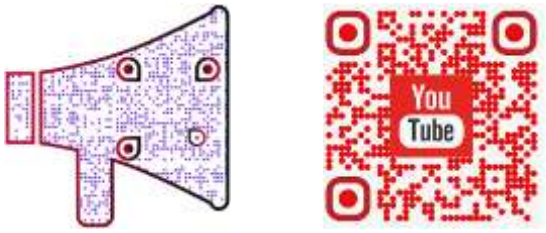
- stores alphanumeric data;

- reads in two directions (horizontally and vertically);

- ability to read from long distance;

- more versatile and customizable in different shapes, colors, sizes, logos and stickers (Fig. 1);

- are read by any smartphone camera application.



a) b)

Figure 1: Types of two-dimensional QR code:
a) QR code with different shape, color and size;
b) QR code with embedded logo

Advantages of two-dimensional coding:

Some marketers misuse QR codes, as result, some people avoid them.

It is also proposed to distinguish between static and dynamic codes.

Static QR codes are one-time codes and cannot be edited after code is created; it can be command line stored as QR code.

Static QR codes are more suitable for personal purposes or disposable use.

The peculiarity is that such QR codes are suitable for fixed actions, for example, identification of employees encoding Wi-Fi settings; registration for events; transfer of requisites; suitable for one-time advertising campaign, etc.

Advantages of static QR codes include fact that they are convenient because content of code is embedded directly, as when copying into code, without external URL or data address.

Disadvantages of static coding include fact that after code is generated, information will remain static (fixed), and then there is no way to change it.

Dynamic QR codes are codes in which information is updated at any time. A dynamic QR code itself assigns short URL t address link that redirects to target site registered to that URL.

Today, there are applications that provide security services, including URL validation and cryptographic decision-making, as well as applications that guarantee user privacy by maintaining least-privileged permission lists [23].

Such dynamic codes are mainly needed to collect statistics, reviews, marketing campaigns.

The advantages of dynamic QR codes include fact that they:

- code does not change, data that can be sewn into it changes;

- convenient with dynamic QR code, you can personalize "services";

- such QR codes are convenient in access control systems.

Disadvantages of dynamic coding include fact that such QR codes need special tool that will help in creating and managing short links, or you need to use your own development service for coding.

The standard modes of encoding QR codes include four [26]:

- numerical;

- alphanumeric;

- binary;

- Kanji.

However, for efficient data storage; extensions can also be used.

Let's highlight key rules when coding:

1. Rational design – size and style.

The size of QR code is also of great importance and largely depends on where QR code will be used.

The distance between code and scanning device (phone) is one of most important factors when deciding on size.

QR codes of small sizes can often go unnoticed, and perhaps even unscannable.

When printing on small and medium-sized products (for example, business cards or leaflets), codes should be at least 2 x 2 cm, but, better, select necessary size by samples (print and decide).

It is necessary to take into account size of dots in QR code. There are more points as data is added. The more data, more rows and columns are needed, which means that code will have more complex visual structure.

The distance between rows and columns in code must also be taken into account, since it is important to maintain desired distance between points so that they do not merge when actual image for scanning is reduced.

Therefore, it is important to choose QR service capable of generating codes of ideal size.

So, you need QR code generator that will allow you to create and download QR codes in high quality, regardless of design, style, color and other elements of code.

Under rational style of QR-code we will understand color and logo.

For example, logo is great way to personalize QR code.

If we are talking about color, then it is worth remembering that color of foreground of QR code is darker than background color.

The ideal option for scanning is black and white design with maximum contrast.

Bright colors in QR code can be main difference between code, however, it can worsen its readability.

Creating QR code with lot of information and in color design is risky, as it can be unreadable.

2. Testing "content" of QR code.

That is, it is necessary to check in advance that after scanning code, user does not get to broken link, etc.

4. Confidentiality of Information When Using QR-Coding

Nowadays, QR codes are used everywhere.

And privacy remains an important issue, because anything can be programmed into QR code – from collecting data from current location to allowing you to make call or even payment transaction [26].

Sometimes in process of QR code scanning, there is chance that it will redirect to form that asks for additional name and phone number information, and this can carry some risk, since people do not always know with whom they are sharing their information.

QR codes are usually safe and effective way to easily share information with others.

Often, when reading QR code by most scanners, there is automatic transition to link, without requesting permission for additional actions.

Let us dwell on main recommendations in order to prevent involuntary transfer of your personal data.

1. Use QR scanners with advanced functions, where, after reading, program will notify you about all processes "sewn" into code, and user will be able to either cancel some actions on his own, or refuse to follow suspicious link.

2. Use of antivirus programs with functions to check security of QR codes.

3. Need to disable automatic action function when scanning QR code, for example, visiting website, downloading file or connecting to Wi-Fi network.

4. Review URL after crawl process to make sure it's legitimate.

5. Do not enter personal data on site to which you went using "random" QR code.

6. Use reliable services to generate code.

7. Never publish QR codes with confidential information.

So, security of QR code is associated with presence of secure QR code generator.

If we consider first recommendation, it should be clarified that QR code scanner itself does not have security problems and cannot be hacked.

Most QR code generators collect minimum of non-personally identifiable data from users who scan QR codes [25].

Usually, this is data (location, number of scans, scan time and operating system (iOS or Android)) of device used to scan

code, collected using QR codes, visible only to "QR code generator".

QR code generators are safe to use and in some cases include additional security measures such as payments. For example, online banking sites use QR code generator as part of two-factor authentication.

When creating code, you need to make sure that QR code generator complies with GDPR requirements.

The Personal Data Protection Regulation (GDPR) introduces new compliance requirements (GDPR compliance) [27], [28].

Companies that comply with requirements of GDPR are obliged to protect information of customers from any extraneous and unauthorized web pages.

So, according to requirements of GDPR, it is necessary to take appropriate technical and organizational measures to protect personal data from:

- losses, for example, due to equipment failure.

- unauthorized access, e.g. due to insufficient compliance with security requirements in IT.

- unintentional disclosure, for example, due to accidental arbitrary access to personal data from Internet.

For companies, information they "share" with QR generator is confidential.

Secure QR code generator should offer solutions that meet company-level security requirements, including encrypted data that restricts access to personal data, and ensures confidentiality of services.

The GDPR prohibits companies from selling data to unauthorized third-party companies and controlling them.

Conventional QR code generators, both online and in applications that are not GDPR compliant, cannot guarantee their users security of data that is used or distributed.

It is necessary to pay attention to fact that if QR code is used to "go" to web page, then it must be certified with SSL (Secure Socket Layer) – protocol for encrypting data exchanged between client and server.

That is, certificate allows you to navigate web pages with HTTP:/ on HTTPS:/ and informs users that web page provides not only security of their data, but also protects against intruders so that they cannot create fake version of "original" site.

In this paper, we will focus on password protection of QR codes.

A password-protected QR code is convenient way to share content, with ability to regulate and restrict access to confidential contents of QR code.

Password-protected QR codes are QR codes in which information or content stored in QR code can only be accessed and viewed after scanners enter correct password (Fig. 2) [28], [29].

When people scan password-protected QR code, they will first be redirected to web page where they will need to enter QR code password. After entering password, scanners will be able to access and view content stored in QR code [30].

Figure 2: Scan code after entering correct password

Although, password feature can be disabled, which will allow wider audience to access contents of QR code at any time.

Also, in order to make sure that QR code that is used is safe, it is proposed to pay attention to such aspects:

- is QR-code solution which use SOC 2 certified;

- whether it is possible to log in using single sign-on system (SSO login).

SOC 2 certification indicates that processes comply with international practices in field of security [31].

An example of secure QR code generator Beaconstac [32]. Beaconstac screen detects inconsistencies in user crawling behavior, detects phishing URLs, and maintains data health. QR solution is SOC-2 compliant. Beaconstac's QR Code Generator allows you to sort and filter QR codes based on commands, campaigns, milestones, or anything else that helps you better organize your work.

Single sign-on (SSO) is authentication capability that allows users to access multiple applications with single set of login credentials. Enterprises typically use single sign-on to provide easier access to variety of web, on-premises, and cloud applications to improve user experience [33], [34].

SSO is necessary for end-to-end security feature when creating and editing QR code, especially when it comes to large volumes of transactions that cannot be disclosed to everyone.

Therefore, having ability to log on with single sign-on limits sign-on by sending permissions to multiple trusted employees. This provides additional layer of security because it prevents unknown users from logging on.

As result, we highlight key aspects that you need to pay attention to in order to make sure that QR-code is safe:

- compliance with QR codes GDPR;

- web resource is certified according to SSL;

- password protection of QR-code;

- SOC 2 certification;

- providing single sign-on.

5. Conclusion

This work is an overview in field of QR codes and their application. In work, two main types of coding (one-dimensional and two-dimensional) were first analyzed, and as result, their advantages and disadvantages are presented. Then attention was focused on analysis of static and dynamic QR codes with determination of their advantages and disadvantages.

The key rules for coding are given.

The main attention in work is paid to confidentiality of personal data both when using QR codes and when creating them.

The paper contains main recommendations in order to prevent involuntary transfer of their personal data.

Also identified are key aspects that you need to pay attention to in order to make sure that QR-code is secure. The difference between this work and similar ones is that work offers such aspect as SOC 2 certification.

The review identified that security risks often associated with QR code generators are not related to QR code technology, but to end purpose of each QR code.

Thus, to ensure confidentiality, you need to clearly know everything not only about technologies that you use, but also about people with whom you share information.

The review showed that there is no standard mechanism in literature to ensure authenticity and confidentiality of contents of QR code.

6. References

[1] Yong, K. S., Chiew, K. L., & Tan, C. L. (2019). A survey of the QR code phishing: the current attacks and countermeasures. In 2019 7th International Conference on Smart Computing & Communications (ICSCC) (pp. 1-5). IEEE.

[2] Ismail, S., Alkawaz, M. H., & Kumar, A. E. (2021). Quick response code validation and phishing detection tool. In 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 261-266). IEEE.

[3] Taraka Rama Mokshagna Teja, M., & Praveen, K. (2022). Prevention of Phishing Attacks Using QR Code Safe Authentication. In Inventive Computation and Information Technologies (pp. 361-372). Springer, Singapore.

[4] Abu-Jassar, A. T., & et al.. (2022). Electronic User Authentication Key for Access to HMI/SCADA via Unsecured Internet Networks. Computational Intelligence and Neuroscience, 2022, Article ID 5866922.

[5] Orobinskyi, P., & et al.. (2020). Comparative Characteristics of Filtration Methods in the Processing of Medical Images. American Journal of Engineering Research, 9(4), 20-25.

[6] Vasiurenko, O., & et al.. (2020). Spatial-Temporal Analysis the Dynamics of Changes on the Foreign Exchange Market: an Empirical Estimates from Ukraine. Journal of Asian Multicultural Research for Economy and Management Study, 1(2), 1-6.

[7] Deineko Zh., & et al.. (2022). QR Code as an Element of Educational Activity. International Journal of Academic Information Systems Research (IJAISR), 6(4), 26-31.

[8] Tvoroshenko, I., & et al.. (2020). Modification of models intensive development ontologies by fuzzy logic. International Journal of Emerging Trends in Engineering Research, 8(3), 939-944.

[9] Babker, A. M., & et al.. (2019). Information technologies of the processing of the spaces of the states of a complex biophysical object in the intellectual medical system health. International Journal of Advanced Trends in Computer Science and Engineering, 8(6), 3221-3227.

[10] Matarneh, R., & et al.. (2019). Improving Fuzzy Network Models For the Analysis of Dynamic Interacting Processes in the State Space. International Journal of Recent Technology and Engineering, 8(4), 1687-1693.

[11] Lyashenko, V., Kobylin, O., & Ahmad, M. A. (2014). General methodology for implementation of image normalization procedure using its wavelet transform. International Journal of Science and Research (IJSR), 3(11), 2870-2877.

[12] Lyashenko, V. (2014). Efficiency of bank crediting of real sector of economy in the context of separate banking groups: an empirical example from Ukraine. International Journal of Accounting and Economics Studies, 2(2), 74-79.

[13] Ahmad, M. A., & et al.. (2020). Interactive Geoinformation Three-Dimensional Model of a Landscape Park Using Geoinformatics Tools. International Journal on Advanced Science, Engineering and Information Technology, 10(5), 2005-2013.

[14] Baranova, V., & et al.. (2020). Price Environment for Gold and Silver in the Context of the Development of COVID-19. Journal of Asian Multicultural Research for Economy and Management Study, 1(2), 25-32.

[15] Pogorelenko, N., & et al.. (2016). Wavelet Coherence as a Research Tool for Stability of the Banking System (The Example of Ukraine). Modern Economy, 7(09), 955.

[16] Lakshmi, G. V., & et al.. (2021). BlockChain based inventory management by QR code using open CV. In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[17] Mathivanan, P., & et al.. (2018). QR code based patient data protection in ECG steganography. Australasian physical & engineering sciences in medicine, 41(4), 1057-1068.

[18] Beck, T., & et al.. (2022). Big techs, QR code payments and financial inclusion (No. 17297). CEPR Discussion Papers.

[19] Deineko, Zh., Sotnik, S., & Lyashenko, V. (2022). Usage and Application Prospects QR Codes. International Journal of Engineering and Information Systems (IJEAIS), 6(7), 40-48.

[20] Barron, I., & et al.. (2020). Dual modulated QR codes for proximal privacy and security. IEEE Transactions on Image Processing, 30, 657-669.

[21] Lin, P. Y., & et al.. (2022). A confidential QR code approach with higher information privacy. Entropy, 24(2), 284.

[22] Wahsheh, H. A., & Al-Zahrani, M. S. (2021). Secure real-time computational intelligence system against malicious QR code links. International Journal of Computers, Communications and Control, 16(3), 1-9.

[23] Wahsheh, H. A., & Luccio, F. L. (2020). Security and privacy of QR code applications: a comprehensive study, general guidelines and solutions. Information, 11(4), 217.

[24] Ebner, M. (2008). QR Code-the Business Card of Tomorrow?. In Proceeding FH Science Day (pp. 431-435). Shaker-Verlag GmbH.

[25] Singh, A. (2019). Smart Library Management System using QR code.

[26] Ave, H., Pkw, B., & Ave, C. (2021). QR code.

[27] Day, G. (2021). Cybersecurity Predictions 2021. ITNOW, 63(1), 10-11.

[28] Alessi, M., & et al.. (2019). A decentralized personal data store based on ethereum: Towards GDPR compliance. Journal of Communications Software and Systems, 15(2), 79-88.

[29] Tjahyadi, S. (2021). Development Of QR Code-Based Data Sharing Web Application Using System Development Life Cycle Method. Journal of Information System and Technology, 2(2), 64-73.

[30] How to create a password-protected QR code (2022). qrcode-tiger-tiger.com.

[31] Clark, R. (2018). Compliance!= security (except when it might be). In Enigma 2018 (Enigma 2018).

[32] Kundaragi, M. S., Halburgi, M. S., & Kaladagi, M. U. (2021). Effective use of QR code technology for library and information services: a special reference to BLDE (Deemed to be University) Vijayapura.

[33] Ratakonda, B., Therala, A., & Hanumanthu, C. K. (2020). Driving license detection using QR code. In E3S Web of Conferences (Vol. 184, p. 01010). EDP Sciences.

[34] Morakinyo O. E. (2021). A secure bank login system using a multi-factor authentication.