СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ ПРИ ПРИМЕНЕНИИ QR-КОДА

Бородина Е.А.,
старший преподаватель
Полтавского национального технического
университета имени Юрия Кондратюка,
Украина, г. Полтава
Швыдкый А.А.,
студент 402-ТН,
Полтавского национального технического
университета имени Юрия Кондратюка,
Украина, г. Полтава
Кикоть А.С.
студентка 401-ТН,
Полтавского национального технического
университета имени Юрия Кондратюка,
Украина, г. Полтава

EXISTING PROBLEMS WHEN USING A QR CODE

Borodina E.A.
Senior lecturer,
Poltava National Technical Yuri Kondratyuk University
Shvidkiy A.A.
student 402-TN,
Poltava National Technical Yuri Kondratyuk University
Kikot A.S.
student 401-TN,
Poltava National Technical Yuri Kondratyuk University

Аннотация

Применении QR-кода упрощает процесс сбора, обработки и хранения информации, однако в свою очередь существует ряд проблем связанных с повреждением кода и возможности получения информации из поврежденного QR-кода. Также необходимо помнить, что в некоторых сферах жизни применение QR-кода может влиять на безопасность и защищенность персональных данных.

Abstract

The use of QR code simplifies the process of collecting, processing and storing information, but in turn there are a number of problems associated with code corruption and the possibility of obtaining information from a corrupted QR code.

It should also be remembered that in some areas of life, the use of QR code can affect the security and security of personal data.

Ключевые слова: QR-код, безопасность, защищенность, исправление ошибок.

Keywords: QR code, security, safety, error correction.

A QR Code is a two-dimensional barcode that is readable by smartphones. It allows to encode over 4000 characters in a two dimensional barcode. QR Codes may be used to display text to the user, to open a URL, save a contact to the address book or to compose text messages [1].

QR codes do have error correction. This error correction can ensure that a QR Code remains readable when as much as 30% of the code is corrupt. In this example, red ink covers a chunk of the QR Code but the QR Code can still be read successfully (figure 1).

Figure 1. QR Code with 30% of squares covered

Error correction is always enabled to some extent, you can't turn it off. When a code is being created, it's down to the designer to specify which of the 4 different levels of error correction they want. The designer can select from the following [3]:

1. L[ow] – up to 7% damage
2. M[edium] – up to 15% damage
3. Q[uality] – up to 25% damage
4. H[igh] – up to 30% damage

Error correction comes at a cost, after all nothing is free, and that cost is that the higher the level of Error correction you apply to your QR Code, the more space you lose to store actual data.

There are times when error correction is worth sacrificing storage space and times when it isn't. For example, on a business card when you likely don’t need to store tonnes of detail, but where the card could become damaged or wet before

the recipient has had a chance to scan it, higher levels of Error Correction could save the day. On the other hand, if you're creating a code that will only be displayed digitally, it's unlikely the content of the code will be damaged and the original is easily reproducible so error correction isn't really very useful, especially not at the highest levels [3].

The content of a QR Code cannot be changed once generated. What is sometimes referred to as a Dynamic QR Code, is a QR Code pointing to a static URL that hosts the actual content (e.g. the real URL). The hosted content can be changed after the QR Code has been printed.

There are however some areas in which QR Codes can pose a risk to your security and safety.

The first and probably main method would be phishing. Phishing isn't just limited to e-mails, viruses or Trojans. In fact due to the appearance of QR Codes, they can be an easy way to target unsuspecting users.

Let's picture, a user sees a poster from their bank with an advert for a great new service they are offering, they trust the bank. The offer is for a limited time only, so the user uses the chance to get more info. The poster proposes a QR Code which promises to take them straight to where they can take advantage of the offer. The person scans the code and he's taken to a website as promised, only what he doesn't realize is that he's been taken to a replica website that's identical in appearance to the bank's intended destination only not actually hosted by the bank. The user proceeds to sign up entering all their account details only to find the following day someone has gained access to their account because of the info they entered in that website. So how is this possible?

It's not as complicated as one may think. The reason this sort of thing can occur is because QR Codes are only meant to be machine readable. This means that a human looking at the code is unable to determine its content, or more importantly identify if it's been manipulated post production. All a scammer would need to do is create a QR Codes of the same dimensions as the one in the poster that contains a link to the fake website they setup in advance, and cover the original QR Code in the posted with the new altered one. Maybe not everyone will fall for it, but many unsuspecting bargain hunters would scan the fake code rather than the one in the original poster. Their trust for their bank may make them less likely to question anything.

References

1. What is a QR Code?. Available at: https://www.the-qrcode-generator.com/whats-a-qr-code

2. How Secure is a QR Code?. Available at: http://qrcode.meetheed.com/question10.php

3. QR Code Error Correction. Available at: http://qrcode.meetheed.com/question17.php?s=s

4. QR code. Available at: https://en.wikipedia.org/wiki/QR_code#Error_correction