

Quick Response-Code (QR-Code)

You can use QR codes to pay invoices, access a digital menu in a restaurant or visit a website. Any data encoded in the code cannot be read by humans. You should therefore be careful when using them.

How to protect yourself when using QR codes:

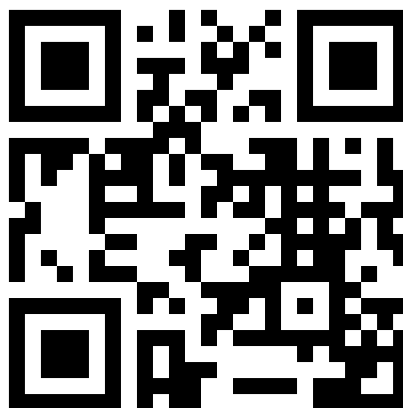
- Only ever use QR code scanners (apps) which show you the content of the code first and don't process it straight away.
- Always check the link destination or payment information after scanning any QR code before opening the target page or completing a transaction.
- Never enter your log-in information on any website you have accessed via a QR code.
- Never allow anyone to talk you into payments via QR codes.
- Only ever use QR codes in situations you consider standard or safe.
- Only use your financial institution's app to pay [QR invoices \(https://www.ebas.ch/qrinvoices\)](https://www.ebas.ch/qrinvoices).

A story of success

QR codes are used more and more widely. Originally, they were used to mark assemblies and components in the car manufacturing sector. The abbreviation "QR" stands for "quick response".

Nowadays, QR codes are also used on invoices ([QR invoice \(https://www.ebas.ch/qrinvoices\)](https://www.ebas.ch/qrinvoices)) or in the publishing and marketing sectors to link physical objects (products, print media, posters, etc.) with the online world and make additional information available this way.

As the contents of QR codes cannot readily be decoded by humans, these codes have to be scanned in first, e. g. using a smartphone or a special reader.



Example QR code by "eBanking – but secure!" (linking to the [www.ebas.ch \(https://www.ebas.ch\)](https://www.ebas.ch) website)

QR codes are easy to use and cheap to produce. No particular resources or technical know-how is required for their

creation. You can generate QR codes on numerous websites. Next to classic QR codes, there is also a trend to generate customised and creative QR codes meant to attract additional attention and serve as advertising.



Example of a creative coloured QR code (of the [NCSC \(https://www.ncsc.admin.ch\)](https://www.ncsc.admin.ch))

Risks involved in using QR codes

These squares can be used to store any information, from simple links to instructions for a banking transaction. With the relevant apps, these are easy to read and are even processed automatically quite often. This plus the fact that users cannot usually establish what a QR code contains before it is read is increasingly abused by fraudsters – especially in view of the fact it is rather easy to create a QR code, for instance by simply taping over an authentic payment code. All payments initiated by scanning the taped-over QR code end up directly on the fraudster's account and not the one of the original recipient.

There is also an increase in [phishing mails \(https://www.ebas.ch/en/phishing\)](https://www.ebas.ch/en/phishing) containing QR codes. These serve to hide links leading to harmful websites from antivirus software and potential victims. A QR code can also hide a link which might for instance lead to a malicious file or app, a dubious app store or an untrustworthy Wi-Fi hotspot.

You should therefore only use a QR code scanner (app) which displays the decoded contents first and asks whether you would actually like to visit a link or execute a certain action. Unfortunately, this is not the case with all mobile devices with an integrated camera app. There are several good apps to be found in official stores which can be installed for this purpose though.

A QR code is a square matrix made up of black and white, sometimes also coloured squares or dots representing various data such as Internet addresses or payment details in binary form. A special marker in three of the four corners of the square indicates its orientation.