



Four Precautions On QR Code Fraud

🔒 cyber security fraud protection

Summary: The use of QR codes has skyrocketed since the pandemic. This year, one billion smartphones are expected to access QR codes globally, according to Juniper Research. This increased use has gotten the attention of cybercriminals. Here are four ways you and your customers can protect yourselves.

Transformers, a species of robotic beings that can change from robots to high-speed vehicles, weapons, or electronic items, were first introduced to the public in 1984 as a Japanese toy line. But they took on a life of their own in 1985 when Hasbro bought the line and partnered with Marvel Comics to create a storyline around the individual toys. The characters became so popular that they spawned a film line, with the first Transformer film coming out in 2007. This film franchise has netted more than \$4.9B in global box office sales, as of 2021.

The idea of things being other than what they appear may be fun in comic books and movies, but not necessarily in the real world. This is something that consumers and financial institutions are discovering first-hand with scammers. Scammers have become increasingly creative and deceptive. They have transformed their tactics to include things people are unlikely to question, such as QR codes. For community financial institutions (CFIs) working to stay on top of banking risks, it is important to stay abreast of this latest type of fraud.

The pandemic triggers QR code growth

With the onset of the pandemic, the use of QR codes surged. As we know, restaurants were at the forefront of QR code adoption with contactless digital menus. In 2020, 52% of US restaurants had switched to QR code menus and likely many more have done so by now. QR code adoption has continued to grow as people become more familiar with its use and costs can be lowered for businesses that use them. This year, [one billion smartphones are expected to access QR codes globally](#), according to Juniper Research.

Financial institutions' use of QR codes

As financial institutions (FIs) need to keep pace with fintechs, many have found QR codes helpful. They streamline the customer experience and can be a secure payment option. With a QR code, customers can be directed to the exact website location for their needs, whether that is for loan documents or opening a new account. Some FIs are using QR codes in place of biometrics and passwords to access their accounts or withdraw funds at an ATM too. This can be a secure and seamless way to access their accounts, but only if the QR codes have end-to-end encryption built in. Venmo, Apple Pay, and PayPal use QR codes and are linked to many FI accounts for payment.

Fake QR codes

The growth of QR codes has not been lost on criminals. They are creating fraudulent QR codes, as a way of redirecting consumers to phony websites to hijack payments, steal passwords, and personal data. They can also be used to reveal a person's location and gain entry into financial accounts.

For instance, in January 2022, authorities in Texas discovered phony QR codes on parking meters in both Austin and Houston. Unsuspecting people were scanning the QR code to make a parking payment and some of them may have been scammed.

While the practice is only just picking up speed, it has been effective enough to make it onto the Federal Bureau of Investigation’s radar. The agency issued a [public service announcement](#), warning people to be vigilant in their use of QR codes.

How to protect your customers from QR code fraud

While we have not heard of any FIs experiencing security issues in their use of QR codes yet, diligence is needed. Educating your customers on the potential risks with QR codes and the latest QR scams will help keep them protected.

1. **Pay attention.** Look first to see if the QR code is on a permanent sign or is a professionally branded sticker. If it seems out of place or tampered with, then don’t scan it. If possible, type in the URL instead of scanning, especially when payments are involved.
2. **Be wary of QR codes in emails.** Just as emails with links should cause anyone to pause, so should QR codes embedded in emails. If you are using QR codes in an email to process transactions or help your customers open accounts, notify them ahead of time that the email is coming. Some scams send an email from a company stating that a payment wasn’t successful and ask you to use the QR code to complete the payment. If your customer recently made a payment to this company, they should call the company directly to confirm the authenticity of the email.
3. **Use a secure scanner app.** This type of app indicates malicious code in QR codes before your phone opens them. There are several free options out there from well-known antivirus companies. Make sure your customer recognizes the company brand, before downloading the app.
4. **Download apps directly.** QR codes can be used to download apps. But, the safest is to download apps directly from a company’s website or the phone’s app store.

As with all technology offerings, QR codes provide benefits and risks. If your institution and your customers stay informed of the risks, you can all enjoy the benefits.

LOOKING TO GROW YOUR LOAN PORTFOLIO?

Financial institutions are looking for ways to boost their loan portfolio. Depending on your portfolio concentration, you may need C&I loans or choose a hedging solution to satisfy the long-term, fixed-rate needs of your customers. Check out our [Lending Services](#) to find the right solution for your institution.

ECONOMY & RATES

Rates As Of: 03/17/2022 12:36PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.44	0.09	0.38
6M	0.86	0.17	0.67
1Y	1.26	0.26	0.87
2Y	1.94	0.50	1.20
5Y	2.18	0.45	0.91
10Y	2.21	0.38	0.69

30Y	2.50	0.33	0.59
FF Market		FF Disc	IORB
0.08		0.50	0.40
SOFR		Prime	QBER
0.05		3.50	0.07

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.