QRurb Your Enthusiasm 2021:

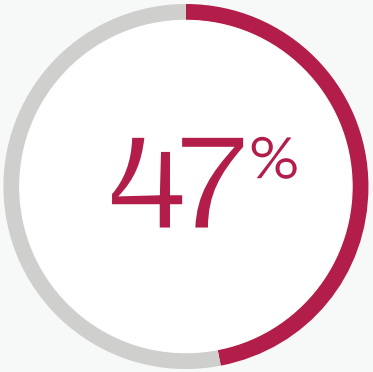
Why the QR code remains a top security threat and what you can do about it

QR codes: Where they started and where they're going

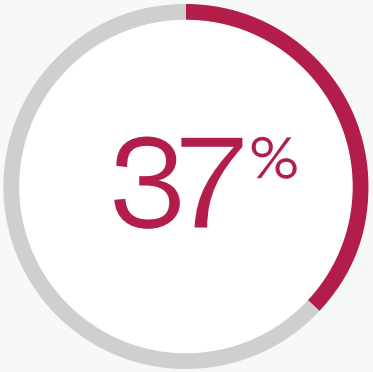
In 2020, we documented the rising use — and potential security risks — of quick response (QR) codes. Although QR codes have been around for decades, their use surged during the COVID-19 pandemic as contactless transactions became the norm around the world. Thanks to QR codes, consumers increasingly used them to access websites, submit orders and make payments while government authorities could use them to facilitate contact tracing and visitor processing at border checkpoints. QR codes made all these cashless, paperless exchanges possible when the world needed them most.

Fast forward to 2021 — what, if anything, has changed?

We know that QR codes are more widespread than ever. Consider that social media platforms now enable users to instantly follow accounts just by scanning a QR code. In addition, QR codes are now practically ubiquitous across China, and South Korea and India have experienced rapid adoption as well. In addition, QR code payment solutions will soon be rolled out across Ghana, Russia and Sri Lanka, and more countries are expected to enable the technology in the coming year.



of respondents were aware that a QR code can open a URL versus 61% in September 2020.



of respondents were aware that a QR code could download an application, down from 49% in the previous survey.

What does the QR code security forecast look like in 2021?

To be honest, based on our survey results, not great. As we noted in our 2020 report, security threats do not lie in the actual QR code itself, but in the lack of consumer awareness about actions QR codes can take without the user knowing. Risky consumer habits, coupled with the general lack of zero trust security on mobile devices, has not improved the mobile threat landscape over the past several months.

Overall, our 2021 survey uncovered these general trends:

- QR code usage is increasing but the knowledge of what they can do lags far behind.
- QR code use cases have expanded and now extend to personal business such as financial transactions and healthcare access.
- These two trends — expanded QR code use and lack of user awareness — may potentially put both consumers and organizations at greater risk of data breaches.

It's clear that QR codes are here to stay, so how can IT security professionals protect their organizations against these vulnerabilities? The rest of this report takes a closer look at global QR code trends and provides insights organizations can use to fortify their security strategies going forward.

Is the world still enthusiastic about QR

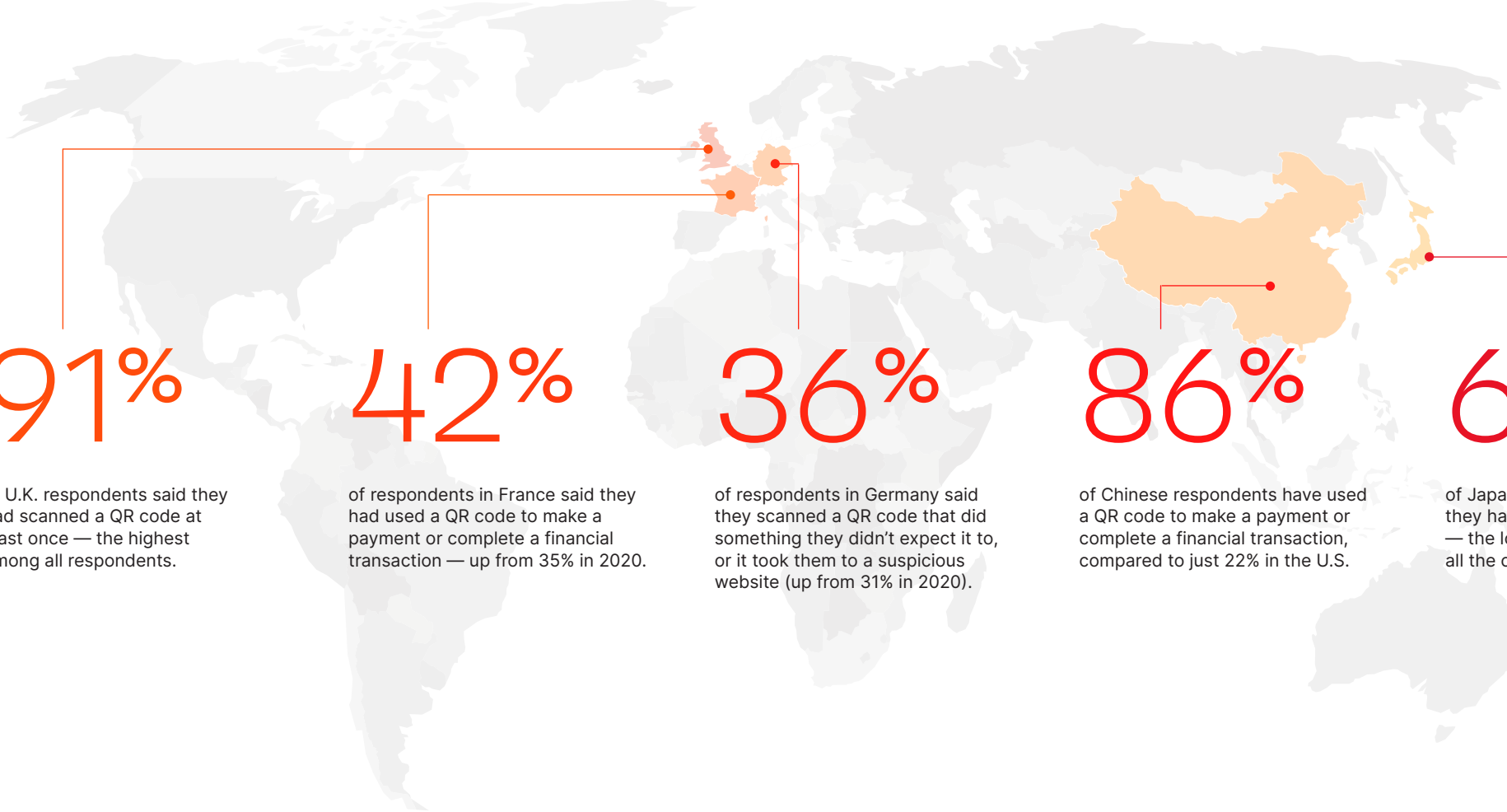
Among the countries we surveyed, we found that China's adoption of QR codes vastly outpaced that of every other country. For instance, China has rapidly embraced QR codes for all activities, while other countries mainly use them to expedite transactions in restaurants, bars and cafes. Interestingly, more than 40% of Chinese respondents said they have scanned a QR code in the past six months for financial reasons, such as accessing a bank account, credit card statement or ATM. By comparison, only 7% of U.S. respondents said they used QR codes for financial transactions.

What's truly curious about this year's findings is that Japan — where QR codes were invented decades ago to streamline automotive assembly — has been slower to adopt QR codes compared to other countries. In fact, only 61% of Japanese respondents said they have ever scanned a QR code, the lowest percentage of all the countries we surveyed.

Perhaps most notable is that the use of QR codes in the U.S. seems to be waning. Less than one-third of respondents said they had scanned a QR code in the past week compared to 39% in 2020.

The number of people who said they had scanned a QR code in the past month dropped by 10 percentage points — from 66% in 2020 to just 56% in the beginning of 2021.

While the reasons behind the downward trend in the U.S. remain unclear, consumer trust in QR codes is trending upward overall — presenting more opportunities for cybercriminals to potentially exploit and misuse this technology.



91%

of U.K. respondents said they had scanned a QR code at least once — the highest among all respondents.

42%

of respondents in France said they had used a QR code to make a payment or complete a financial transaction — up from 35% in 2020.

36%

of respondents in Germany said they scanned a QR code that did something they didn't expect it to, or it took them to a suspicious website (up from 31% in 2020).

86%

of Chinese respondents have used a QR code to make a payment or complete a financial transaction, compared to just 22% in the U.S.

61%

of Japanese respondents said they had scanned a QR code — the lowest percentage of all the countries surveyed.

Does increased trust lead to increased risk from QR codes?

Although our survey found varying rates of adoption across countries, trust in QR codes increased across the board. In many cases, consumers expressed fewer worries and less awareness about the potential security risks of QR codes. For instance, 2021 survey respondents were less concerned about privacy (51%) and financial breaches (46%) compared to 2020, when 58% of respondents had privacy concerns and more than half (51%) had financial concerns. Additionally, overall awareness of actions QR codes can take, such as opening a URL, sending a text, or revealing the user's location, was down across all categories.

The fact that only about half (51%) of users don't have, or don't know if they have, security software installed on their mobile devices means IT organizations must prioritize security against malicious QR codes in 2021.

As a result, it's not surprising that more consumers are using QR codes for personal business without giving security much thought. In fact, 83% of respondents stated that they used a QR code to make a payment or complete a financial transaction in the last year. Of those respondents, 54% had used a QR code for a financial reason in the past three months alone. This dramatic increase could be due to decreased security concerns, as well as the normalization of contactless payments during the pandemic.

However, here's the truly worrisome revelation for security: Although use of QR codes is declining overall among consumers, QR codes are being used to access more sensitive information, such as credit card information, bank accounts, and healthcare records. At the same time, QR codes are more frequently taking actions the user didn't expect or worse — directing them to malicious websites. This, combined with the fact that only about half (51%) of users don't have, or don't know if they have, security software installed on their mobile devices means IT organizations must prioritize security against malicious QR codes in 2021.

83%

of respondents stated that they used a QR code to make a payment or complete a financial transaction in the last year. Of those respondents, 54% had used a QR code for a financial reason in the past three months alone..

47%

of respondents were aware that a QR code can open a URL versus 61% in 2020 — a decrease of 14 percentage points.

37%

of respondents were aware that a QR code could download an application, down nearly 12 percentage points from 2020.

How has the mobile threat landscape changed?

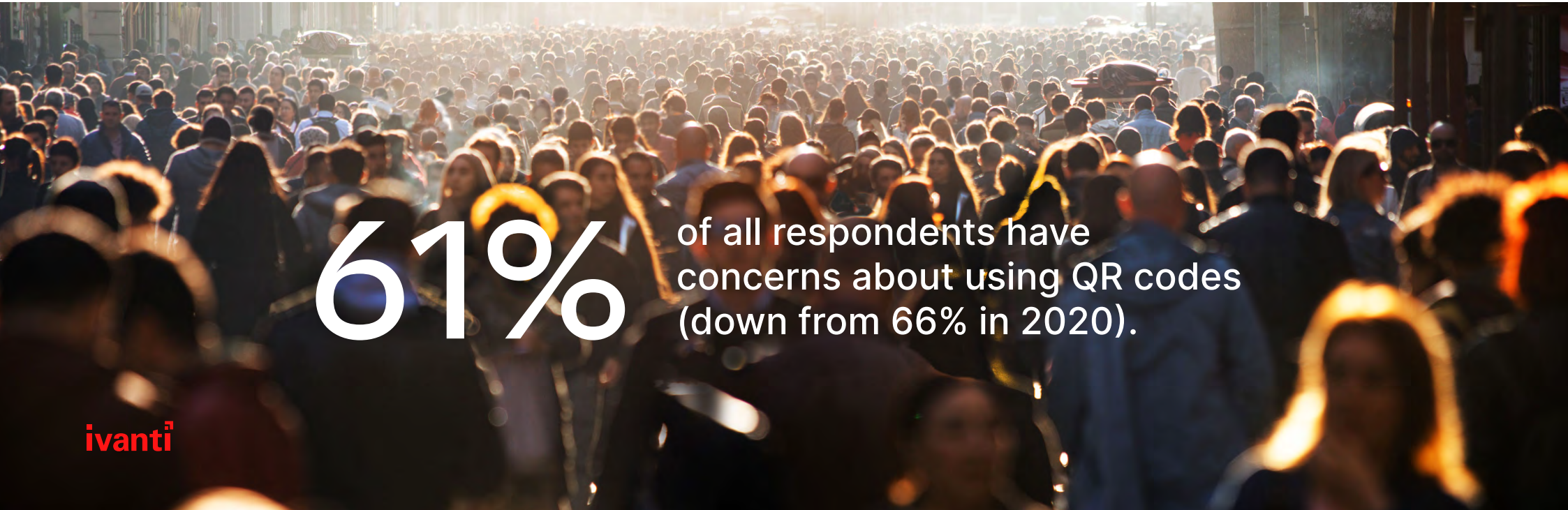
As our research has shown, less than half of consumers worldwide have mobile security on their devices. Cybercriminals are also aware of this fact, which is why they've shifted their tactics to target mobile users, who are generally less secure and more distracted than corporate PC users. The use of QR codes to execute malicious attacks on mobile devices has been documented as far back as 2013, when it was clear that hackers were linking QR codes to websites embedded with malware. The malicious website would infect the device with a Trojan, which then unleashed surveillance and data exfiltration attacks and sent this information back to the hacker's servers.

Not much has changed since then, except that QR codes are now much more widely used in 2021 than in 2013, and for more transactions. This, combined with the general lack of consumer awareness about how QR codes work still makes them an incredibly useful tool for hackers.

Nowadays consumers may unwittingly scan fraudulent QR codes, which takes them to a legitimate-looking website that prompts users to provide data such as username and password, credit card information, company login and more. The cybercriminal then uses this information to access the user's accounts or corporate apps and data that may be on the device.

And, just like Trojans of the past, in 2021 QR codes can still be used to download malicious software onto a mobile device without the user knowing.

Although the techniques have changed and continue to evolve, the goal is the same: to gain access to valuable data. This is why it's more important than ever to have a mobile security foundation that can protect against these evolving threats.



Threat protection requires mobile security and user education

It's no surprise that hackers are continuing to use QR codes to gain access to mobile devices, apps and data. This is largely because QR codes are cheap and easy to generate and exploit. A combination of consumer education, good security hygiene and a robust mobile security platform can help minimize — or even eliminate — these risks altogether.

What users can do

- Never trust emails from unknown senders (which is a good security practice in general).
- Treat unknown QR codes the same as unknown URLs, which is essentially what they are.
- Make sure the QR code is the original and not pasted over with another one if located on a physical location such as a store display.
- Use QR scanner software to view the URL before clicking on it.

ivanti

What companies can do

As mentioned previously, users typically have no idea if any kind of security exists on their mobile devices. To be honest, that's how it should be. Remote employees should be able to stay productive without having to constantly update security software or enter passwords to access company apps and data.

Zero trust mobile security that validates every device, user, app, URL, network and cloud is critical for protecting against phishing and other malicious exploits that leverage QR codes to bypass traditional antivirus software. Specifically, organizations need a complete mobile device management and security platform that can discover, manage and secure every device that accesses business resources.

With the ability to see and protect every device across your everywhere workplace, you can defend against phishing attacks as well as device, app and network threats — even when devices aren't connected to the network. And, by expanding the use of multi-factor authentication, companies can also eliminate passwords — one of the top causes of phishing-related data breaches.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

I. [Report overview]
II. In September 2020, MobileIron (acquired by Ivanti in December 2020) conducted an ambitious survey of nearly 4,500 consumers across the U.S., U.K., Germany, Netherlands, France and Spain. (The results of that report can be found here.) At the start of 2021, Ivanti expanded the survey to include consumers in China and Japan, which replaced Spain and the Netherlands in the survey. The current study offers a broader picture of how QR codes are being used beyond the U.S. and western Europe — giving security professionals more insight into global QR code trends.