QRurb Your Enthusiasm 2021:

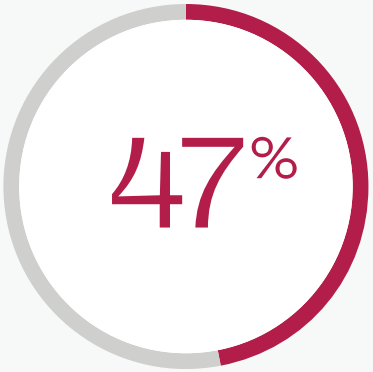
Warum der QR-Code eine Top-Sicherheitsbedrohung bleibt und was Sie dagegen tun können

QR codes: Wie alles anfing und wohin die Reise geht

Im Jahr 2020 dokumentierten wir die steigende Nutzung – und potenzielle Sicherheitsrisiken – von Quick Response (QR)-Codes. Obwohl es QR-Codes schon seit Jahrzehnten gibt, stieg ihre Nutzung während der COVID-19-Pandemie sprunghaft an, als kontaktlose Transaktionen auf der ganzen Welt zur Norm wurden. Dank der QR-Codes nutzten Verbraucher sie zunehmend, um auf Webseiten zuzugreifen, Bestellungen aufzugeben und Zahlungen zu tätigen, während staatliche Behörden sie zur Erleichterung der Kontaktverfolgung und der Besucherabfertigung an Grenzkontrollstellen nutzen konnten. QR-Codes machten all diese bargeldlosen, papierlosen Transaktionen möglich, als die Welt sie am meisten brauchte.

Spulen wir ins Jahr 2021 vor – was, wenn überhaupt, hat sich verändert?

Wir wissen, dass QR-Codes weiter verbreitet sind als je zuvor. Man bedenke, dass Social Media Plattformen wie Facebook, Snapchat, Twitter, LinkedIn und Instagram es den Nutzern nun ermöglichen, Accounts sofort zu folgen, indem sie einfach einen QR-Code scannen. Außerdem sind QR-Codes in China mittlerweile praktisch allgegenwärtig, und auch in Südkorea und Indien ist die Akzeptanz sehr hoch. Darüber hinaus werden QR-Code-Bezahllösungen bald in Ghana, Russland und Sri Lanka eingeführt, und es wird erwartet, dass weitere Länder die Technologie im kommenden Jahr einführen werden.



der Befragten waren sich bewusst, dass ein QR-Code eine URL öffnen kann, im Vergleich zu 61% im September 2020.

der Befragten wussten, dass man mit einem QR-Code eine Anwendung herunterladen kann, im Vergleich zu 49% in der vorherigen Umfrage.

Wie sieht die Prognose für die QR-Code-Sicherheit im Jahr 2021 aus?

Um ehrlich zu sein, basierend auf unseren Umfrageergebnissen, nicht sehr gut. Wie wir in unserem Bericht 2020 festgestellt haben, liegen die Sicherheitsbedrohungen nicht im eigentlichen QR-Code selbst, sondern im mangelnden Bewusstsein der Verbraucher über Aktionen, die QR-Codes ohne das Wissen des Nutzers durchführen können. Riskante Verbrauchergewohnheiten, gepaart mit dem allgemeinen Mangel an Zero-Trust-Sicherheit auf mobilen Geräten, haben die mobile Bedrohungslandschaft in den letzten Monaten nicht verbessert.

Insgesamt hat unsere Umfrage 2021 diese allgemeinen Trends aufgedeckt:

- Die Nutzung von QR-Codes nimmt zu, aber das Wissen darüber, was sie tun können, hinkt weit hinterher.
- Die Anwendungsbereiche von QR-Codes haben sich erweitert und erstrecken sich nun auch auf persönliche Geschäfte wie Finanztransaktionen und Zugang zum Gesundheitswesen.
- Diese beiden Trends – die erweiterte Nutzung von QR-Codes und das mangelnde Bewusstsein der Nutzer – können sowohl Verbraucher als auch Unternehmen einem größeren Risiko von Datenschutzverletzungen aussetzen.

Es ist klar, dass QR-Codes nicht mehr wegzudenken sind. Wie also können IT-Sicherheitsexperten ihre Organisationen vor diesen Schwachstellen schützen? Der Rest dieses Berichts wirft einen genaueren Blick auf die globalen QR-Code-Trends und liefert Erkenntnisse, die Unternehmen nutzen können, um ihre Sicherheitsstrategien in Zukunft zu stärken.

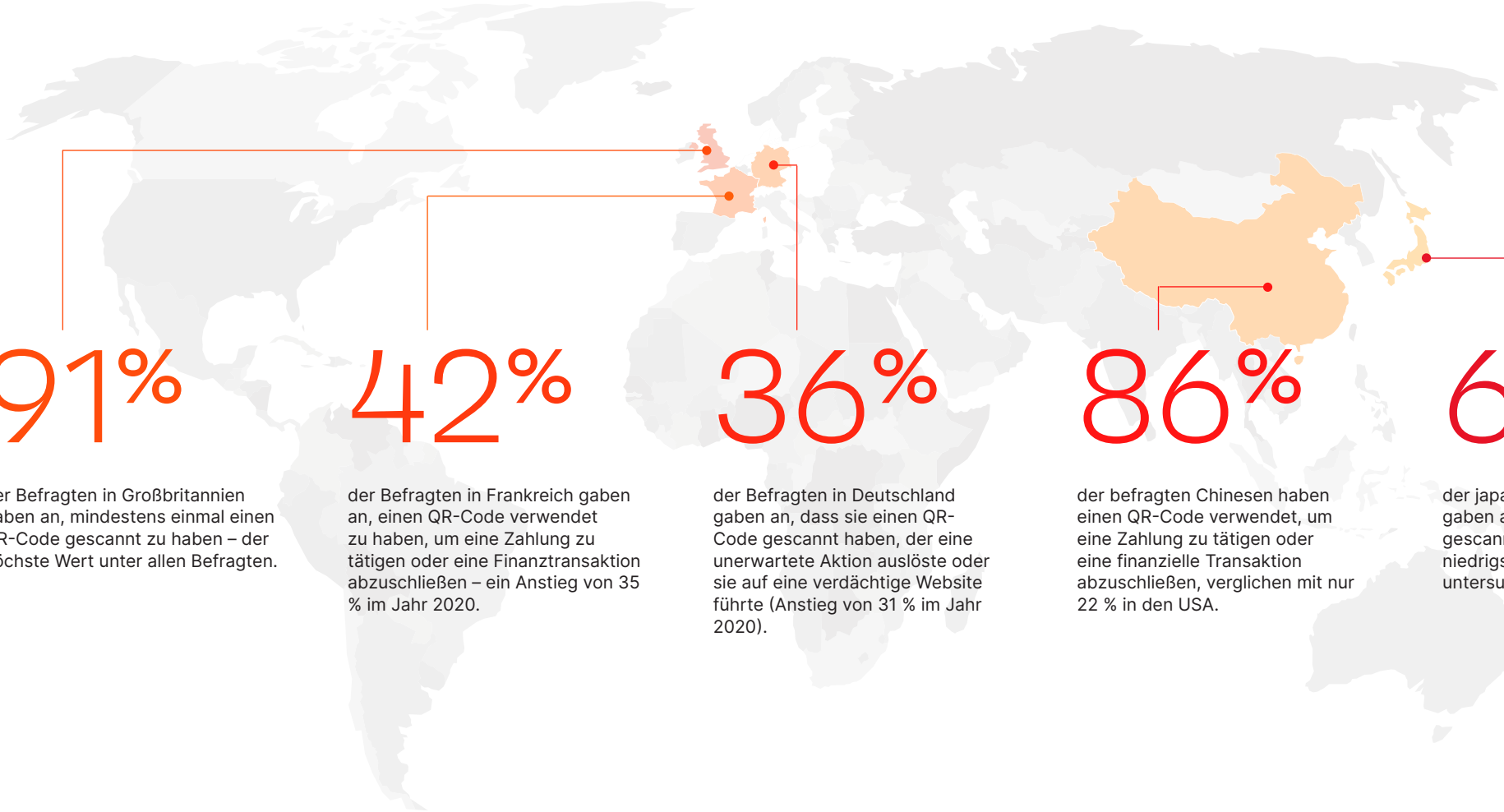
Ist die Welt noch begeistert von QR-Codes?

Unter den von uns untersuchten Ländern haben wir festgestellt, dass die Akzeptanz von QR-Codes in China die aller anderen Länder bei weitem übertrifft. Zum Beispiel hat China QR-Codes schnell für alle Aktivitäten eingeführt, während andere Länder sie hauptsächlich zur Beschleunigung von Transaktionen in Restaurants, Bars und Cafés verwenden. Interessanterweise gaben mehr als 40 % der befragten Chinesen an, dass sie in den letzten sechs Monaten einen QR-Code aus finanziellen Gründen gescannt haben, z. B. um auf ein Bankkonto, eine Kreditkartenabrechnung oder einen Geldautomaten zuzugreifen. Im Vergleich dazu gaben nur 7% der US-Befragten an, QR-Codes für finanzielle Transaktionen zu nutzen.

Was wirklich kurios an den diesjährigen Ergebnissen ist, ist, dass Japan – wo QR-Codes vor Jahrzehnten erfunden wurden, um die Automobilmontage zu rationalisieren – im Vergleich zu anderen Ländern langsamer bei der Einführung von QR-Codes war. Tatsächlich gaben nur 61 % der japanischen Befragten an, schon einmal einen QR-Code gescannt zu haben, der niedrigste Prozentsatz aller von uns untersuchten Länder.

Am bemerkenswertesten ist vielleicht, dass die Verwendung von QR-Codes in den USA abzunehmen scheint. Weniger als ein Drittel der Befragten gab an, in der letzten Woche einen QR-Code gescannt zu haben, verglichen mit 39 % im Jahr 2020. Die Zahl der Personen, die angaben, im vergangenen Monat einen QR-Code gescannt zu haben, sank um 10 Prozentpunkte – von 66 % im Jahr 2020 auf nur noch 56 % Anfang 2021.

Während die Gründe für den Abwärtstrend in den USA unklar bleiben, steigt das Vertrauen der Verbraucher in QR-Codes insgesamt an – was Cyberkriminellen mehr Möglichkeiten bietet, diese Technologie potenziell auszunutzen und zu missbrauchen.



91%

der Befragten in Großbritannien gaben an, mindestens einmal einen QR-Code gescannt zu haben – der höchste Wert unter allen Befragten.

42%

der Befragten in Frankreich gaben an, einen QR-Code verwendet zu haben, um eine Zahlung zu tätigen oder eine Finanztransaktion abzuschließen – ein Anstieg von 35 % im Jahr 2020.

36%

der Befragten in Deutschland gaben an, dass sie einen QR-Code gescannt haben, der eine unerwartete Aktion auslöste oder sie auf eine verdächtige Website führte (Anstieg von 31 % im Jahr 2020).

86%

der befragten Chinesen haben einen QR-Code verwendet, um eine Zahlung zu tätigen oder eine finanzielle Transaktion abzuschließen, verglichen mit nur 22 % in den USA.

61%

der japanischen Befragten gaben an, einen QR-Code gescannt zu haben – der niedrigste Prozentsatz aller untersuchten Länder.

Führt erhöhtes Vertrauen zu einem erhöhten Risiko durch QR-Codes?

Obwohl unsere Umfrage in den einzelnen Ländern unterschiedliche Akzeptanzraten ergab, stieg das Vertrauen in QR-Codes in allen Ländern. In vielen Fällen äußerten die Verbraucher weniger Bedenken und ein geringeres Bewusstsein über die potenziellen Sicherheitsrisiken von QR-Codes. So waren die Umfrageteilnehmer 2021 weniger besorgt über Datenschutzverletzungen (51 %) und finanzielle Sicherheitslücken (46 %) im Vergleich zu 2020, als 58 % der Befragten Bedenken in Bezug auf den Datenschutz und mehr als die Hälfte (51 %) in Bezug auf finanzielle Sicherheitslücken hatten. Darüber hinaus war der Bekanntheitsgrad von Aktionen, die QR-Codes auslösen können, wie z. B. das Öffnen einer URL, das Versenden eines Textes oder die Preisgabe des Standortes des Nutzers, über alle Kategorien hinweg rückläufig.

Die Tatsache, dass nur etwa die Hälfte (51 %) der Nutzer keine Sicherheitssoftware auf ihren mobilen Geräten installiert hat oder nicht weiß, ob sie eine solche haben, bedeutet, dass IT-Organisationen im Jahr 2021 der Sicherheit vor bösartigen QR-Codes Priorität einräumen müssen.

Daher ist es nicht verwunderlich, dass immer mehr Verbraucher QR-Codes für persönliche Geschäfte nutzen, ohne sich über die Sicherheit Gedanken zu machen. Tatsächlich gaben 83 % der Befragten an, dass sie im letzten Jahr einen QR-Code verwendet haben, um eine Zahlung zu tätigen oder eine finanzielle Transaktion abzuschließen. Von diesen Befragten haben 54 % allein in den letzten drei Monaten einen QR-Code aus einem finanziellen Grund verwendet. Dieser dramatische Anstieg könnte auf verringerte Sicherheitsbedenken sowie auf die Normalisierung des kontaktlosen Bezahlens während der Pandemie zurückzuführen sein.

Doch hier ist die wirklich besorgniserregende Enthüllung in Bezug auf Sicherheit: Obwohl die Nutzung von QR-Codes bei den Verbrauchern insgesamt rückläufig ist, werden QR-Codes verwendet, um auf sensiblere Informationen zuzugreifen, wie z. B. Kreditkarteninformationen, Bankkonten und Gesundheitsdaten. Gleichzeitig führen QR-Codes immer häufiger Aktionen aus, die der Benutzer nicht erwartet hat, oder schlimmer noch – sie leiten ihn auf bösartige Websites. Zusammen mit der Tatsache, dass nur etwa die Hälfte (51 %) der Nutzer keine Sicherheitssoftware auf ihren mobilen Geräten installiert hat oder nicht weiß, ob sie eine solche installiert hat, bedeutet dies, dass IT-Organisationen im Jahr 2021 der Sicherheit vor bösartigen QR-Codes Priorität einräumen müssen.

83%

der Befragten gaben an, dass sie im letzten Jahr einen QR-Code verwendet haben, um eine Zahlung zu tätigen oder eine finanzielle Transaktion abzuschließen. Von diesen Befragten haben 54 % allein in den letzten drei Monaten einen QR-Code aus einem finanziellen Grund verwendet.

47%

der Befragten wussten, dass ein QR-Code eine URL öffnen kann, gegenüber 61 % im Jahr 2020 - ein Rückgang um 14 Prozentpunkte.

37%

der Befragten wussten, dass über einen QR-Code eine Anwendung heruntergeladen werden kann, ein Rückgang von fast 12 Prozentpunkten gegenüber 2020.

Wie hat sich die mobile Bedrohungslandschaft verändert?

Wie unsere Untersuchungen gezeigt haben, haben weniger als die Hälfte der Verbraucher weltweit mobile Sicherheitslösungen auf ihren Geräten. Auch Cyberkriminelle sind sich dieser Tatsache bewusst und haben deshalb ihre Taktik auf mobile Benutzer verlagert, die im Allgemeinen weniger sicher und abgelenkter sind als PC-Benutzer in Unternehmen. Die Verwendung von QR-Codes zur Ausführung bösartiger Angriffe auf Mobilgeräte wurde bereits 2013 dokumentiert, als klar wurde, dass Hacker QR-Codes mit Websites verlinkten, in die Schadsoftware eingebettet war. Die bösartige Website infizierte das Gerät mit einem Trojaner, der dann Überwachungs- und Datenexfiltrationsangriffe auslöste und diese Informationen zurück an die Server des Hackers schickte.

Seitdem hat sich nicht viel geändert, außer dass QR-Codes im Jahr 2021 viel häufiger verwendet werden als im Jahr 2013 und für mehr Transaktionen. Dies, zusammen mit dem allgemeinen Mangel an Verbraucherbewusstsein darüber, wie QR-Codes funktionieren, macht sie immer noch zu einem unglaublich nützlichen Werkzeug für Hacker.

Heutzutage kann es vorkommen, dass Verbraucher unwissentlich betrügerische QR-Codes scannen, die sie auf eine legitim aussehende Website führen, auf der Benutzer aufgefordert werden, Daten wie Benutzernamen und Passwort, Kreditkarteninformationen, Firmenlogin und mehr anzugeben. Der Cyberkriminelle verwendet diese Informationen dann, um auf die Konten des Benutzers oder auf Unternehmens-Apps und -Daten zuzugreifen, die sich möglicherweise auf dem Gerät befinden. Und genau wie Trojaner in der Vergangenheit können auch im Jahr 2021 QR-Codes verwendet werden, um Schadsoftware auf ein mobiles Gerät herunterzuladen, ohne dass der Benutzer davon weiß.

Obwohl sich die Techniken verändert haben und weiterentwickelt werden, ist das Ziel das gleiche: Zugang zu wertvollen Daten zu erhalten. Aus diesem Grund ist es wichtiger denn je, eine mobile Sicherheitsgrundlage zu haben, die vor diesen sich entwickelnden Bedrohungen schützen kann.

Schutz vor Bedrohungen erfordert mobile Sicherheitslösungen und Benutzerschulung

Es ist keine Überraschung, dass Hacker weiterhin QR-Codes nutzen, um Zugang zu mobilen Geräten, Apps und Daten zu erhalten. Das liegt vor allem daran, dass QR-Codes billig und einfach zu erzeugen und zu nutzen sind. Eine Kombination aus Verbraucheraufklärung, guter Sicherheitshygiene und einer robusten mobilen Sicherheitsplattform kann helfen, - diese Risiken zu minimieren oder sogar - ganz zu eliminieren.

Was Benutzer tun können

- Vertrauen Sie niemals E-Mails von unbekannten Absendern (was generell eine gute Sicherheitspraxis ist).
- Behandeln Sie unbekannte QR-Codes genauso wie unbekannte URLs, was sie im Grunde auch sind.
- Vergewissern Sie sich, dass der QR-Code das Original ist und nicht mit einem anderen überklebt wurde, wenn er sich an einem physischen Ort befindet, z. B. an einem Ladendisplay.
- Verwenden Sie eine QR-Scanner-Software, um die URL anzuzeigen, bevor Sie sie anklicken.

ivanti

Was Unternehmen tun können

Wie bereits erwähnt, haben Benutzer in der Regel keine Ahnung, ob auf ihren mobilen Geräten irgendeine Art von Sicherheitsvorrichtung existiert. Um ehrlich zu sein, so sollte es auch sein. Remote-Mitarbeiter sollten in der Lage sein, produktiv zu bleiben, ohne ständig Sicherheitssoftware aktualisieren oder Passwörter eingeben zu müssen, um auf Firmen-Apps und -Daten zuzugreifen.

Zero Trust Security für Mobilgeräte, die jedes Gerät, jeden Benutzer, jede App, jede URL, jedes Netzwerk und jede Cloud validiert, ist entscheidend für den Schutz vor Phishing und anderen bösartigen Exploits, die QR-Codes ausnutzen, um herkömmliche Antiviren-Software zu umgehen. Konkret benötigen Unternehmen eine vollständige Plattform für die Verwaltung und Sicherheit mobiler Geräte, die jedes Gerät, das auf Unternehmensressourcen zugreift, erkennen, verwalten und sichern kann.

Mit der Möglichkeit, jedes Gerät an Ihrem gesamten Arbeitsplatz zu sehen und zu schützen, können Sie Phishing-Angriffe sowie Geräte-, App- und Netzwerkbedrohungen abwehren – auch wenn die Geräte nicht mit dem Netzwerk verbunden sind. Und durch die Ausweitung des Einsatzes von Multi-Faktor-Authentifizierung können Unternehmen auch Passwörter eliminieren – eine der Hauptursachen für Phishing-bedingte Datenverletzungen.

ivanti

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

I. [Report overview]
II. Im September 2020 führte MobileIron (im Dezember 2020 von Ivanti übernommen) eine ambitionierte Umfrage unter fast 4.500 Verbrauchern in den USA, Großbritannien, Deutschland, den Niederlanden, Frankreich und Spanien durch. (Die Ergebnisse dieses Berichts finden Sie hier.) Zu Beginn des Jahres 2021 erweiterte Ivanti die Umfrage um Verbraucher in China und Japan, die Spanien und die Niederlande in der Umfrage ersetzten. Die aktuelle Studie bietet ein breiteres Bild darüber, wie QR-Codes über die USA und Westeuropa hinaus genutzt werden – und gibt Sicherheitsexperten mehr Einblick in globale QR-Code-Trends.