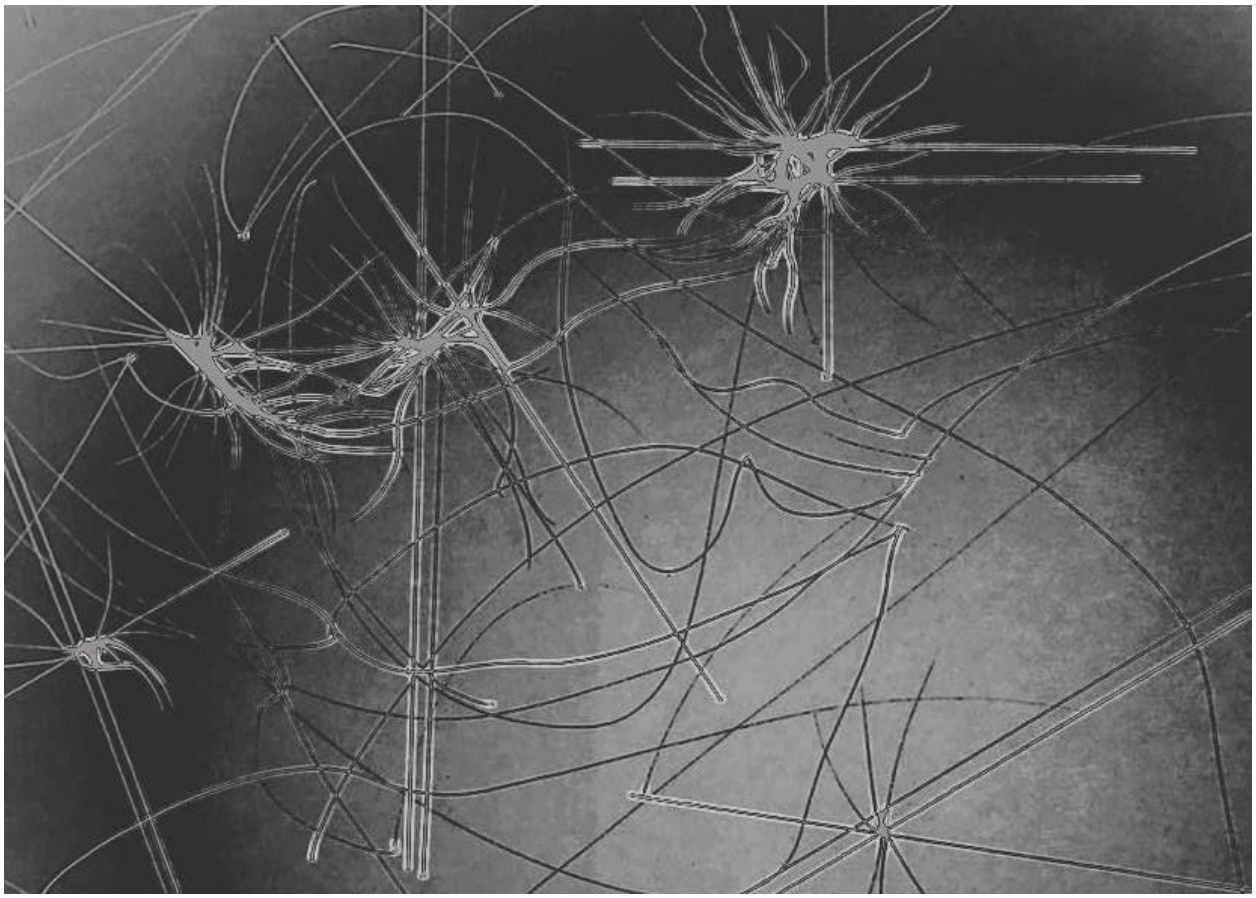
The Hidden Danger of QR Codes



I am very glad that you are reading my article again, dear friends! It would seem, what danger can a QR code pose? It turns out that you can even lose your cryptocurrency as well as fiat money and internet logins because of several attacks, which are based on the mechanics of QR codes.

Let's study these attacks and see how we can successfully defend against them!

In this article, I will be referring to various amazing Authors and resources I strongly recommend that you separately study them on your own. The references list is at the end of the article, enjoy reading!

#Special Thanks:

- ***Much thanks Peachs for help with editing & proofreading!***
- **Much thanks a Deer from Telegram for help with proofreading!**

#I - What is a QR code?

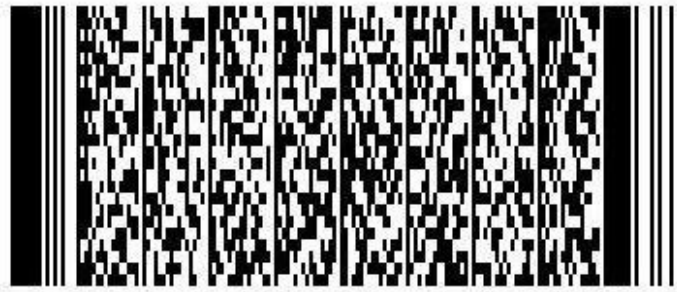
A QR code is a two-dimensional barcode that can store 7,089 digits or 4,296 characters. It can be scanned using a QR code scanner or reader, which is built into most mobile devices' default cameras, to decipher the data that's encoded into it.

This is a string of text, and it's typically a URL or link to a website or a merchant's official account on a payment system. Scanning a QR code saves a user the trouble of typing out a long address in a web browser or manually entering a merchant's username or number in a payment app, among other advantages.

According to Kody Kinzie, a Security researcher, the answer to the limitation of linear barcodes was 2D barcodes, which offer more storage resistance to having physical damage affect the information contained within. Some of the first 2D codes looked like the one below, which is still widely used today.

Aztec code is a 2D, or matrix, machine-readable code that is similar in many ways to a QR code and can hold more information than a linear barcode. Initially developed for logistics, you may see it used on packages and envelopes when more data needs to be stored than a linear barcode can provide.

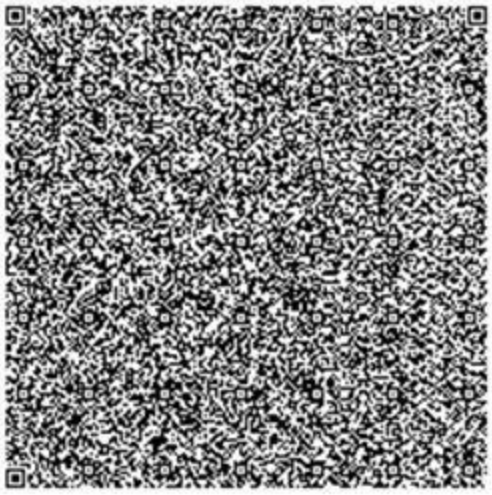
Other types of 2D barcodes can contain an extremely dense amount of data. The PDF417 format found on the back of most driver's licenses in the United States, for example, can encode up to 1800 ASCII characters.



PDF417 codes like the above can encode text, numbers, files, and actual data bytes, and they're more resistant to errors than linear barcodes. Companies like FedEx use a combination of PDF417 and other barcodes on packing slips to automate delivery and tracking.

QR codes started in the automotive industry as a way to keep track of cars as they were being manufactured but quickly grew in popularity outside that industry. Similar to other 2D codes, QR codes can pack a ton of data and can even work when reduced in resolution or otherwise damaged.

One fascinating application of QR codes enabled by their larger data capacity is using them to manage Wi-Fi connections without sharing the password in plain text. By encoding the following string, you can create a QR code that logs Android users into a Wi-Fi network automatically.



The convenience QR codes offer and the ubiquity of mobile devices have contributed greatly to the widespread use of these two-dimensional barcodes. However, their popularity has also created fertile ground for malicious actors to spruce up their

QR code malware toolkit to steal not only personal information but also hard-earned assets that are impossible to recover once lost. Threats involving QR codes have become so rife and sly that the FBI has recently issued a warning about them.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 04, 2021

Alert Number
I-110421-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

The FBI warns the public of fraudulent schemes leveraging cryptocurrency ATMs and Quick Response (QR) codes to facilitate payment. The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions.

A QR code is a square barcode with information that can be scanned and read with a smartphone camera. An individual can scan the QR code of an intended recipient to auto-populate the recipient field making it easier to send cryptocurrency to the correct destination. QR codes can be used at cryptocurrency ATMs to direct payment to an intended recipient. While many businesses have legitimately used QR code payment in the last year because of the COVID-19 pandemic, QR codes also play a role in malicious use of cryptocurrency payments.

Criminal actors, in various fraudulent schemes, maliciously leverage cryptocurrency ATMs and QR codes to receive payments from victims. Such schemes include online impersonation schemes (scammer falsely identifies as a familiar entity such as the government, law enforcement, a legal office, or a utility company), romance schemes (scammer establishes an online relationship with a victim by creating a false sense of intimacy and dependency), and lottery schemes (scammer falsely convinces a victim that they have won an award and consequently demands the victim to pay lottery fees).

Regardless of the scheme, the methods using cryptocurrency ATMs and QR codes appear similar. The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts, such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction. The scammer then directs the victim to a physical cryptocurrency ATM to insert their money, purchase

As the agency describes it, the scammer will contact their victim and somehow convince them that they need to send money, either with promises of love, further riches, or by impersonating an actual institution like a bank or utility company.

After the mark is convinced, the scammer will have them get cash (sometimes out of investment or retirement accounts), and head to an ATM that sells cryptocurrencies and supports reading QR codes. Once the victim is there, they'll scan a QR code that the scammer sent them, which will tell the machine to send any crypto purchased to the scammer's address.

Just like that, the victim loses their money, and the scammer has successfully exploited them.

account overseas. This differs from traditional bank transfers or wires where a payment transaction can remain pending for one to two days before settlement. It can also make law enforcement's recovery of the funds difficult and can leave many victims with a financial loss.

Tips to Protect Yourself:

- Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.
- Do not follow instructions from someone you have never met to scan a QR code and send payment via a physical cryptocurrency ATM.
- Do not respond to a caller, who claims to be a representative of a company, where you are an account holder, and who requests personal information or demands cryptocurrency. Contact the number listed on your card or the entity directly for verification.
- Do not respond to a caller from an unknown telephone number, who identifies as a person you know and requests cryptocurrency.
- Practice caution when an entity states they can only accept cryptocurrency and identifies as the government, law enforcement, a legal office, or a utility company. These entities will likely not instruct you to wire funds, send checks, send money overseas, or make deposits into unknown individuals' accounts.
- Avoid cryptocurrency ATMs advertising anonymity and only requiring a phone number or e-mail. These cryptocurrency ATMs may be non-compliant with US federal regulations and may facilitate money laundering. Instructions to use cryptocurrency ATMs with these specific characteristics are a significant indicator of fraud.
- If you are using a cryptocurrency ATM and the ATM operator calls you to explain that your transactions are consistent with fraud and advises you to stop sending money, you should stop or cancel the transaction.

The FBI Victim Services Division is responsible for ensuring that victims of crimes investigated by the FBI are afforded the opportunity to receive the notification and services as required by federal law and the Attorney General Guidelines for Victim and Witness Assistance. Victim Specialists are highly trained professionals who assess victims' needs to determine what types of services and resources will be most helpful. For more information, please visit www.fbi.gov/resources/victim-services.

If you believe you have been a victim of a cryptocurrency ATM or QR code scam, report the fraud to your local FBI field office. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov.

Malicious actors seek out ordinary, unsuspecting people who don't know much, if at all, about QR code safety. So, how does one avert QR code scams?

In this article, I will discuss with you the various ways fraudsters use QR codes to deceive users and recommend tips on how users can protect themselves from QR code scams.

First of all, let's define what attacks exist and we will start with the very first one that comes to mind - an attack on the money in the bank account where cryptocurrencies and QR is only a tool.

Don't be discouraged - there are more serious attacks to come, but I want you to understand that government agencies rarely pay so much attention to such a seemingly

insignificant type of scam. Maybe there is a reason to kill this type at its very inception and make people aware of such an attack, through QR.

Let's figure out where it all started! It's important to note that malicious actors have invested a great deal of time and resources in making their QR code-enabled scams seem legitimate and useful, as illustrated by the following examples:

#Overlaid QR Codes

A prime example of a QR code scam that relies on the physical realm has malicious actors printing out QR code stickers and physically placing them over genuine ones. People generally assume that the signs or posters with QR codes in shops and public spaces are safe, and thus might be unaware that malicious actors could replace legitimate QR codes with fake ones as part of their fraudulent schemes.

This was the case in a scheme involving payments for bike sharing in China. Malicious actors reportedly replaced the QR codes that users needed to scan to pay for the use of the bikes before they could be unlocked.

As a result, the payments of unsuspecting users were transferred to the malicious actors' accounts, without the users have been able to unlock the bikes for their use.

Just recently, law enforcement in several US cities issued warnings about a similar scheme, where malicious actors had stuck their fraudulent QR codes onto legitimate ones on__parking meters__ to trick users into entering their payment credentials in their phishing websites.

#QR Codes used in real-world social engineering

Another example of a QR code scam that takes advantage of the physical realm is a scheme that was carried out in a parking lot in the Netherlands and that led to the theft of thousands of euros.

Malicious actors reportedly approached individuals to pay the parking fee not through the designated machine in the parking lot purportedly because it was broken. Wearing professional-looking attire to look more credible, the fraudsters coaxed their victims into scanning the QR code they had instead, thereby diverting the payments to their account.

#QR Codes in phishing emails

Scammers have been known to incorporate QR codes into their phishing attacks, a practice known as "quishing." They do this mainly so that they could bypass traditional

security solutions that can flag malicious URLs when they appear in emails but not when they're linked to (or hidden behind) QR codes.

In December 2021, a phishing campaign that used QR codes to steal the banking credentials of users in Germany was reported. In the campaign, malicious actors send an email impersonating a bank and asking the recipient to review and agree to changes in the bank's privacy policy by scanning the QR code in the email. But the QR code links to a phishing site where the victim can unwittingly enter their banking credentials for the malicious actors to collect.

A quishing scheme to obtain Microsoft 365 credentials was also reported late last year. This campaign begins with an email coming from a previously compromised email account and containing a voicemail message that the recipient can supposedly listen to by scanning the QR code in the email. The QR code, however, leads to a bogus login page designed to steal Microsoft 365 credentials.

#QR Codes for subscribing to premium services

Malicious actors can use QR codes to subscribe unsuspecting users to premium services and steal the funds charged to these users monthly. This scheme was used in the Android trojan campaign known as GriftHorse, which had victimized more than 10 million users around the world by September 2021.

#QR Code and barcode scanner apps

In mid-2021, QR code and barcode scanner apps that linked to the Anatsa malware appeared on Google Play. (They have since been taken down from the store.) Infection with such an app starts with forcing the user to update the app upon installation, apparently so that the user can continue to use it.

After the successful download of the supposed update, the app prompts the user to allow the installation of apps from unknown sources. Since the user was previously made to believe that the update was necessary for the app to work properly, the user grants the permission. Once the update is done, the malware runs on the device and immediately asks the user to grant accessibility service privileges.

Malicious actors gain full control over the device and can perform actions on the user's behalf after the user enables accessibility service privileges. At this point, the malware-infested app runs and operates as a legitimate app. The stage has thus been set for malicious actors to steal login credentials and gain access to all the information that is shown on the unsuspecting user's device.

#QR Code creator apps

Trojanized apps can masquerade as QR code creator apps. In a scheme perpetrated by the malicious actor group Brunhilda, such an app asks the user to register. Once registration is done and it obtains detailed device information, the app downloads and installs a trojan payload, which could carry out the theft of sensitive personal information such as login credentials or bank account details.

#QR codes used in Doxxing

First of all, anyone can create a tracking pixel, link to a page, and then link it to a QR code. Any popular logger (canarytokens.org, iplogger.com) can be used for this purpose if receiving extended data in the logger settings is enabled.

The created pixel also can be placed on an external site. It could be a blog (telegra.ph, medium.com, teletype.in) or even an OSINT source page (start.me) which in turn may be linked to a QR code.

#III - QR Code Bugs & Issues

#Apple IOS 11

With iOS 11, Apple introduced a new feature that gives users the ability to automatically read QR codes using their iPhone's native camera app without requiring any third-party QR code reader app.

You need to open the Camera app on your iPhone or iPad and point the device at a QR code. If the code contains any URL, it will give you a notification with the link address, asking you to tap to visit it in the Safari browser. However, be careful — you may not be visiting the URL displayed to you, security researcher Roman Mueller discovered.

According to Mueller, the URL parser of the built-in QR code reader for the iOS camera app fails to detect the hostname in the URL, which allows attackers to manipulate the displayed URL in the notification, tricking users to visit malicious websites instead.

For the demo, the researcher created a QR code (shown above) with the following URL:

https://xxx\\@facebook.com:443@infosec.rm-it.de/

If you scan it with the iOS camera app, it will show following notification:

Open "facebook.com" in Safari

When you tap it to open the site, it will instead open:

https://infosec.rm-it.de/

There is also a tool which is called a QRGen - it can create malicious QR codes and even encode custom-made payloads. These attacks are potent because humans can't read or understand the information contained in a QR code without scanning it, potentially exposing any device used to attempt to decipher the code to the exploit contained within.

Even QR code scanners like smartphones can be vulnerable to these kinds of attacks, as QR codes were found to be capable of luring iPhone users to malicious sites. Check out this awesome write-up which describes how this tool works in detail.

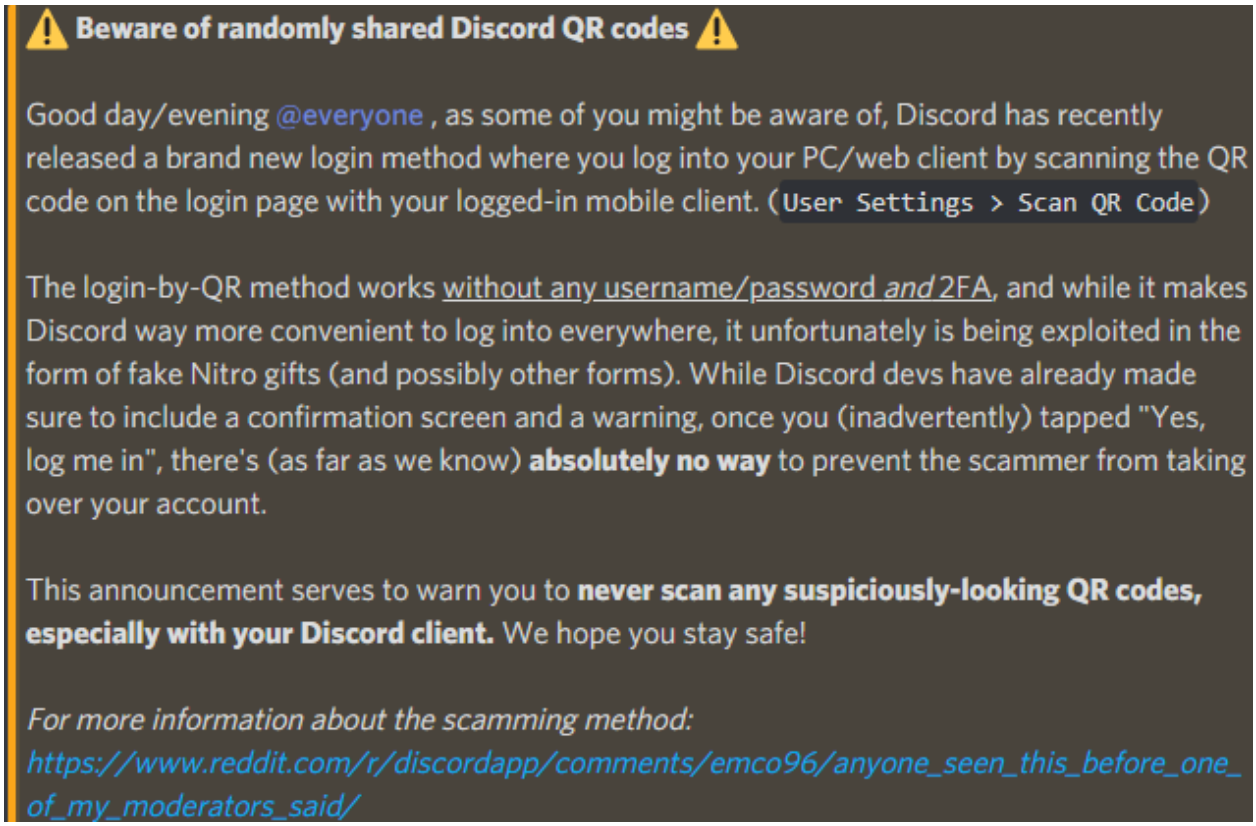
#Discord QR Login

In December 2020, developers at Discord – a voice and text chat app widely used by the gaming community – announced the launch of a QR code feature that enables users to log into the desktop web client using their phone, by scanning the code that appears on-screen.

- **Discord has made some changes to its QR code login system following reports that the mechanism is being abused by scammers trying to gain access to users' accounts.**

While this feature was aimed at simplifying the Discord login process for desktop users, news has surfaced that fraudsters have been exploiting the system to gain unauthorized access to accounts.

According to discussions on various Discord servers and on social media, scammers have been posting QR codes with the promise of free Nitro, the platform's subscription package that offers numerous perks, and other giveaways.



In scanning the code, however, users inadvertently provide the attacker with access to their account.

"The login-by-QR method works without any username/password and 2FA, and while it makes Discord way more convenient to log into everywhere, it, unfortunately, is being exploited in the form of fake Nitro gifts (and possibly other forms)," said one Discord user.

Opinion split over the potential severity of this exploit. For some users, having their accounts compromised may result in little more than frustration – although it's unlikely that anyone would be happy with someone being able to impersonate them online.

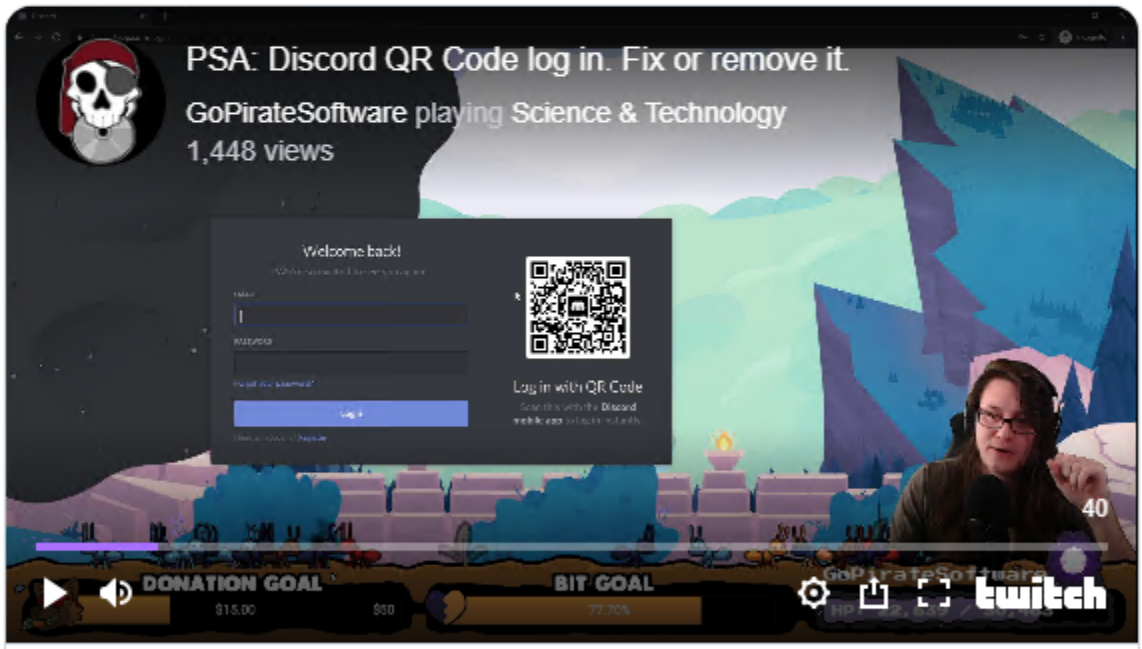
However, after releasing a proof of concept to demonstrate the apparent ease of exploitation, Twitch partner Pirate Software said that if the user was a Nitro subscriber,

an attacker could gain access to their name, address, and [unobfuscated PayPal email address](#).

Pirate Software
@PirateSoftware

Proof of concept for the @discordapp exploit allowing anyone to access your account if you use the phone app to scan their new QR code login system. This bypasses 2FA.

Do not scan QR codes using the Discord phone app. Period.



PSA: Discord QR Code - Clip of GoPirateSoftware - Twitch Clips
Clip of GoPirateSoftware Playing Science & Technology - Clipped by KisaSatoma
clips.twitch.tv

1:07 AM · Jan 13, 2020 · Twitter Web App

218 Retweets **216** Likes

Discord did not immediately respond to our request for comment. The staff weighed in on a Reddit discussion thread, noting that the QR code login window had been reduced, to thwart any would-be scammers.

"We recently reduced the validity window of the QR code from 10 minutes to 2 minutes," said one Discord engineer, who added:

We… noticed an uptick in people trying to socially engineer users into scanning QR codes in an attempt to trick them into logging into another device that they don't control.

Our original thought was that the verbiage on the screen would be enough to deter social engineering attacks, however, we agree that more clear verbiage and a warning could be in place.

Across our mobile app release channels, we have modified the verbiage in the confirmation screen to more clearly emphasize that you are logging into another device, and impose a delay before the 'log me in' button is active (hopefully making people read the red text.) You can see this new screen here.

In addition to being discussed on multiple Discord servers, the issue has already found its way to social media, with one user tweeting: "PSA: If someone sends you a QR code through Discord, don't scan it. They can use it to get instant access to your account."

"A good amount of misinformation being made here," they said. "Discord requires that you confirm the login before the attacker has access. If you just ignore the warnings that Discord gives you, then it's your fault. Just be smart and don't fall for those attacks."

Over on Reddit, however, the 'don't fall for attacks' argument fell short.

“I don’t get the elitism of, ‘If you’re getting phished, it’s your fault, now bugger off, discord should change nothing,” wrote one user. “Create something safe and sound, not, ‘Yeah, that QR code can be used to log in, it clearly said so, but you didn’t pay attention…’”

- **Read How to Avoid Blockchain Blackhats on Discord**

Do we know how many other applications that use QR have this vulnerability? For example, in Telegram? Of course, the question is rhetorical.

#IV - QR + Crypto = ?..

#Keep your Fox Safe!

Scammers may use QR codes to dupe users into downloading counterfeit cryptocurrency wallets by promising that, in doing so, they would get rewards, which are fake tokens. Another kind of bait involves using QR codes to download fake cryptocurrency wallets that promise reductions in miner fees.

Another related scam is the use of QR codes to obtain unauthorized approval of tokens, which are used to facilitate the transfer of assets from one cryptocurrency wallet to another. Incident reports have cited this scheme as the primary reason for the loss of significant funds.

Also, cryptocurrency-related QR code scams involving MetaMask which is a cryptocurrency wallet for interacting with the Ethereum blockchain. Malicious actors can hack into MetaMask extension accounts through QR codes to transfer funds without the account owner's private keys.

- **Read about when after multiple Apes were stolen, MetaMask made changes to its mobile QR Code sync**

“This is incredibly embarrassing on some levels, Nicholas tweeted. “On others, incredibly traumatizing. Yes, I opened up the QR code and sign the ledger. But I was being severely manipulated and didn’t realize what was happening until it was too late. I was scammed, phished, and robbed. Some assholes are going to say ‘that’s what you get.’ And maybe they’re right. But let’s be clear, a scam is a scam, theft is theft, and I had no intention of transferring or selling those assets. So now I am trying to find ways to get my property back.”

- **Read about 6 ways how a website can attack your MetaMask!**

Take look at a new scam method! Do not confuse it with an allowance approve scam (to prevent it you can use revoke.cash / unrekt.net) which targets ERC20 tokens, but not Ethers. (1, 2, 3, 4).

- **Read how hackers may steal your Ethers and why the eth_sign function matter.**

When the people behind the ZenGo wallet wanted to add QR code support, they decided to do a bit of research into the security aspects first. What they found was disturbing – but not entirely unexpected. Anyone can simply generate a QR code that sends money to their address instead of the one intended. And no one can tell as pretty much all QR codes look alike.

#An investigation from ZenGo:

For example, ZenGo used a Googled site to request a QR code for the address: *18Vm8AvDr9Bkvij6UfVR7MerCyrz3KS3h4*, they instead received a QR code that sent funds to the scammer's address: *17bCMmLmWayKGCH678cHQETJFjhBR44Hjx*

Interestingly, they noticed that some scammers have upped the ante with a few tricks. Some of the fake QR code sites manipulated the QR code so that if you checked, it superficially looks like the right address by matching the first letter or numeral such as '1', '3' or 'bc'.

Others muck around with code so that if you try and copy and paste the address to double-check it, the site will copy your address to the clipboard instead of theirs so that you think it matches. ZenGo tracked about $20,000 worth of scammed Bitcoin using the addresses they examined and believed it's just the tip of the iceberg!

I would add that in my opinion here will help the principle of separation of devices - with one clean device with airgap.it you can scan QR, with another only sit on the browser, and on the third most secure cold or paper storage - store basic savings. Nothing prevents you from storing your main "hot sum" on the same split vault. Stay safe!

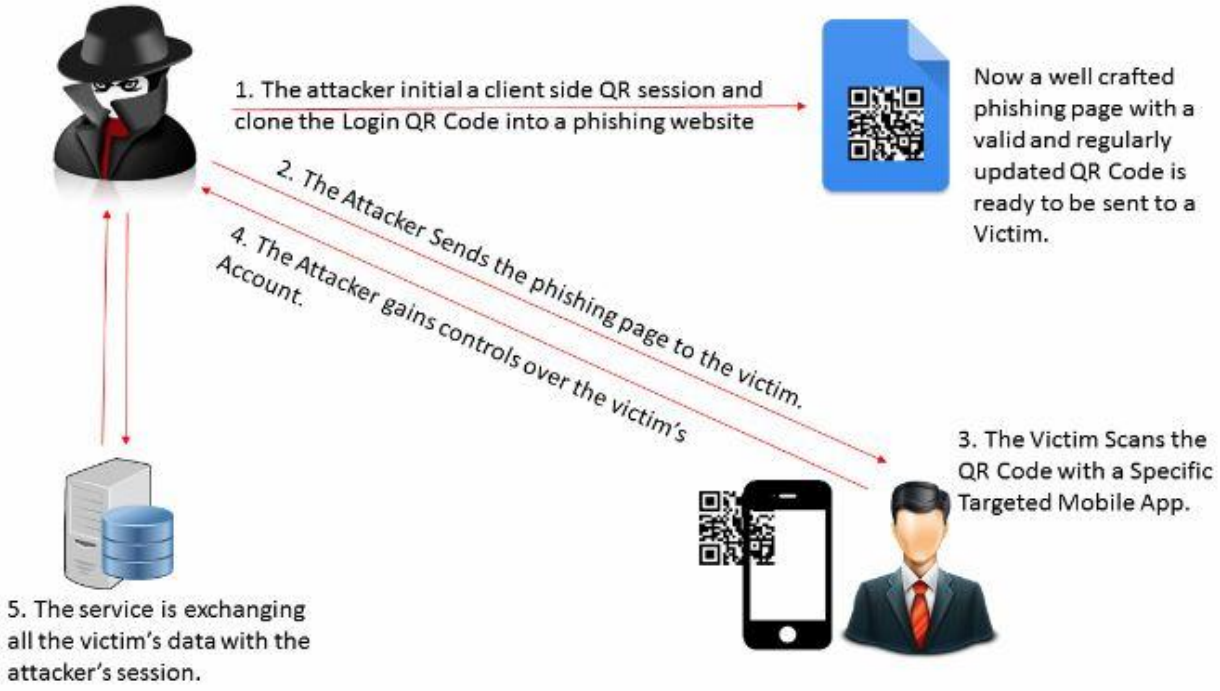
#V - QRLJacking: A review from the OWASP community

QRLJacking or Quick Response Code Login Jacking is a simple social engineering attack vector capable of session hijacking affecting all applications that rely on the "Login with QR code" feature as a secure way to login into accounts. Simply, In a nutshell, the victim scans the attacker's QR code results of session hijacking.

Here's how the QRLJacking attack works behind the scenes:

1. **The attacker initials a client-side QR session and clones the Login QR Code into a phishing website. “Now a well-crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.”**
2. **The Attacker Sends the phishing page to the victim. (refer to [QRLJacking real-life attack vectors])**
3. **The Victim Scans the QR Code with a Specific Targeted Mobile App.**
4. **The Attacker gains control over the victim’s Account.**
5. **The service is exchanging all the victim’s data with the attacker’s session.**

#QRLJacking Attack Flow



For more information on QRLJacking tools and extra, please visit the [QRLJacking on Github]

#Proof of Concept examples (Videos)

- **[WhatsApp QRHijackingVulnerability]**
- **[WhatsApp Accounts Hijacking and ARPpoisoning]**
- **[AirDroid vulnerable to QRLJackingVulnerability]**
- **[Vulnerable Web Applications and Services use Login by QR CodeFeature part #1]**
- **[Vulnerable Web Applications and Services use Login by QR CodeFeature part #2]**

#VI - Tips to ensure QR code safety

While the schemes discussed in this article might seem worrisome, users can keep QR code scams at bay by following these best practices suggested by TrendMicro:

- **Make sure that the linked website of a government agency or other official service provider is legitimate before you provide your personal information. Check for any misspellings on the URL itself.**
- **Think twice before you scan a QR code found in emails that are sent to you even if they seem to come from organizations or people you know. Enable multifactor authentication with your banking, enterprise, and other accounts to prevent theft of login credentials.**
- **When transacting on a merchant or service provider's premises, check the QR code to make sure it's not pasted over an original, legitimate one.**
- **Use QR codes to pay only when you're transacting directly with trusted merchants, service providers, or persons you know.**
- **Be careful about granting permissions when an app asks for them, as some of the requested permissions could be dangerous.**

QR codes can encode a lot of information, and as we've learned today, they can even be formatted to cause a device to perform actions like connecting to a Wi-Fi network. That makes scanning a QR code risky, as a person has no way of reading the information before exposing your device to whatever payload is contained inside.

If you scan a QR code that seems suspicious, pay attention to what the code is attempting to launch, and do not connect to a Wi-Fi network or navigate to a link that's shortened. Some researchers even note the benefit of QR for overall anonymity in blockchain! This means that this technology has a future in Web3.0 as well as it already has in Web2.0.

While most QR codes should be safe to scan on a smartphone, scanning payloads we generated today on a device for scanning tickets or boarding passes may result in some bizarre behavior from the device. Do not scan payloads on a scanner you need working immediately after for an event or work — or any scanner you do not have permission to test — as some of these payloads may cause the scanner to stop working.

I am not asking you to comply with all of this, but you must remember the main rule in this particular case:

- **Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.**

If we finally want to give people the opportunity to be their bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money!

Follow the 25 rules in this set, the first 10 rules relate to personal security, and the rest to corporate security, also keep an eye on the latest trends in crypto OpSec, that always makes sense. Don't be afraid of links, you don't need all of them but you should be able to pick up which will interest you the most for your Pathway.

- **DarkNet-DeepWeb OpSec Guide**
- **ThreatModeling**
- **Read about Timing Attack | Attack via a Representative Sample**

Use extensive measures when working with files and always keep an eye on the latest security trends even if your area is far from it. Take this subreddit and this awesome old & trusted resource as the first step. In our dangerous world, anyone can become a target, especially in crypto.

That said, it doesn't matter what industry you're in. If you have any sensitive, proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind. Also, who knows how many more vulnerabilities lurk in QR codes? Just google QR Code 0day, QR Code 1 day, or QR code CVE and you will see many interesting things - for example, 1, 2.

Learn the latest attack techniques, white-hat cheatsheets, and defense methods, and join hacker communities - because only with knowledge can we defeat the knowledge of hackers. In this intellectual battle, the most prepared will win and I believe that it will be you, Anon. It sounds scary but it is possible, the main thing is to always think ahead.

Forewarned is forearmed! Stay safe!

#References:

- **www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/hidden-scams-in-malicious-scans-how-to-use-QR-codes-safely**
- **null-byte.wonderhowto.com/how-to/create-malicious-QR-codes-hack-phones-other-scanners-0197416/**
- **micky.com.au/how-scammers-are-using-QR-codes-to-steal-your-bitcoin/**
- **threatpost.com/qr-code-scammers-bitcoin-atms/168621/**
- **www.zdnet.com/article/fbi-warning-crooks-are-using-fake-QR-codes-to-steal-your-passwords-and-money/**
- **www.coindesk.com/business/2021/11/05/fbi-warns-of-scams-using-crypto-ATMs-and-QR-codes/**
- **www.theverge.com/2021/11/5/22765900/crypto-scam-FBI-PSA-atm-QR-code-wire-transfer-con-artist**
- **tech.hindustantimes.com/tech/news/iphone-user-beware-of-fake-QR-codes-71651747604570.html**

- securityaffairs.co/wordpress/70739/hacking/qr-code-ios-bug.html
- github.com/h0nus/QRGen

#Check out my articles:

- Key principles of storing crypto, cold wallet security
- 2 violent attack vectors in Crypto: a closer look
- A CIA Agent's Guide to Steganography, Fooling the KGB and Protecting Your Crypto
- OpSec in Crypto & Web3.0: Thoughts
- A View on OpSec Through the Prism of Time
- All known smart contract-side and user-side attacks and vulnerabilities in Web3.0, Defi, NFT, and Metaverse

---

#Support me:

Support is very important to me, with it I can spend less time at work and do what I love — educating Defi & Crypto users! ❤️

- Check out my GitHub
- Track all my activities
- All my Socials
- Join my TG channel

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU — BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds — Monero XMR**