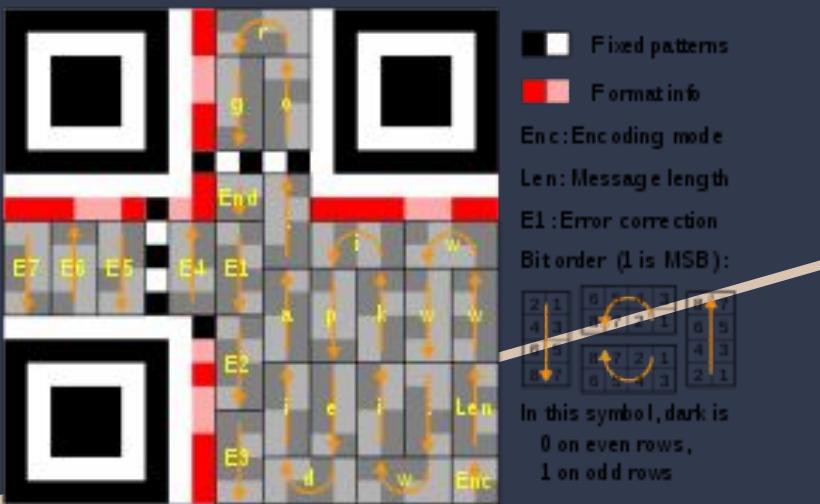




Quick Response (QR) Code Security

Team Members: George Kent-Scheller, John
Kircher, Sam Krasnoff, Julian Padgett

A short background on QR codes



QR codes are a machine-readable code made up of black and white squares for storing URLs and other encoded data.

They can store bytecode which can be used to store, at a maximum, 2953 bytes, which is a very limited amount of code.

Since the beginning of the COVID-19 Pandemic, usage of QR codes has increased to eliminate the need for physical human interaction. This has changed how individuals use and interact with this technology.

Problem Statement

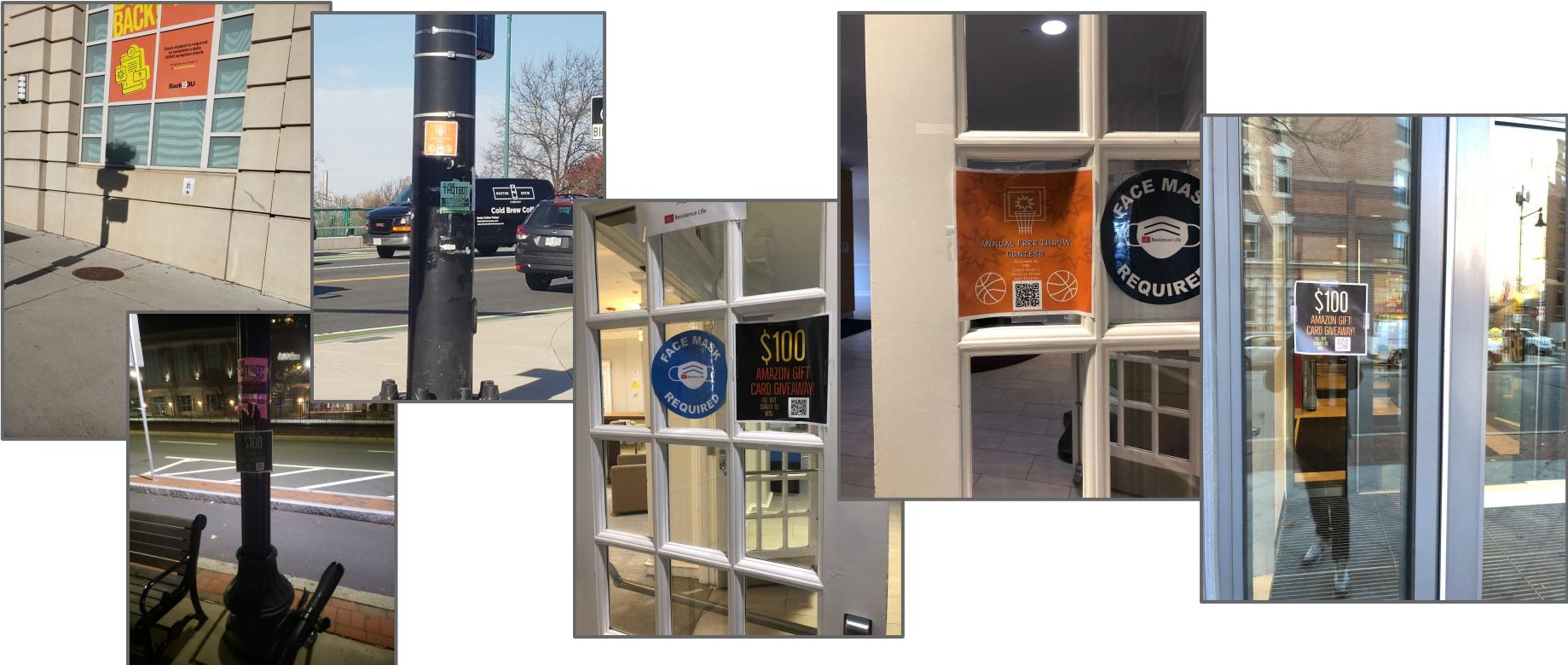
While QR codes have made certain aspects of life more convenient, they aren't secure or safe and can be exploited to create attacks. Given the ubiquity of QR codes today, the way QR codes function must be improved upon to protect people from potential attackers.



Our Experiment: Flyers Around Campus



Flyers Around Campus Continued...



YSSQCYDT (You Shouldn't Scan QR Codes You Don't Trust)

Also you shouldn't click on all links that you see.

QR codes are a media for storing arbitrary information.

They contain no security at all.

Scanning them blindly may leave you vulnerable to:

- Malicious Javascript
- Malware downloads
- BotNets(an attack that uses your computer or phone for its processing power, i.e. to mine bitcoin)
- Man-in-the-middle attack(an attack where the attacker pretends to be the website you expected and steals your inputs and the websites outputs)
- Cross site scripting attacks (an attack that allows websites to steal your cookies)
- Phishing scams
- Cross site Request forgery(an attack that uses your cookies to gain access to a different site you are authenticated to.)
- Arbitrary code execution
- And Many more

We are interested in finding out why you scanned this QR code.

Please fill out the below form to help us get an idea of who you are in the context of our research.

To be clear there is not a \$100 amazon gift card giveaway, that advertising was an attempt to see which source of qr codes people are most likely to click on. Thank you for helping us with our study!

How did you get this link?

What is your level of technical understanding?

(optional)Thoughts on the experiment?

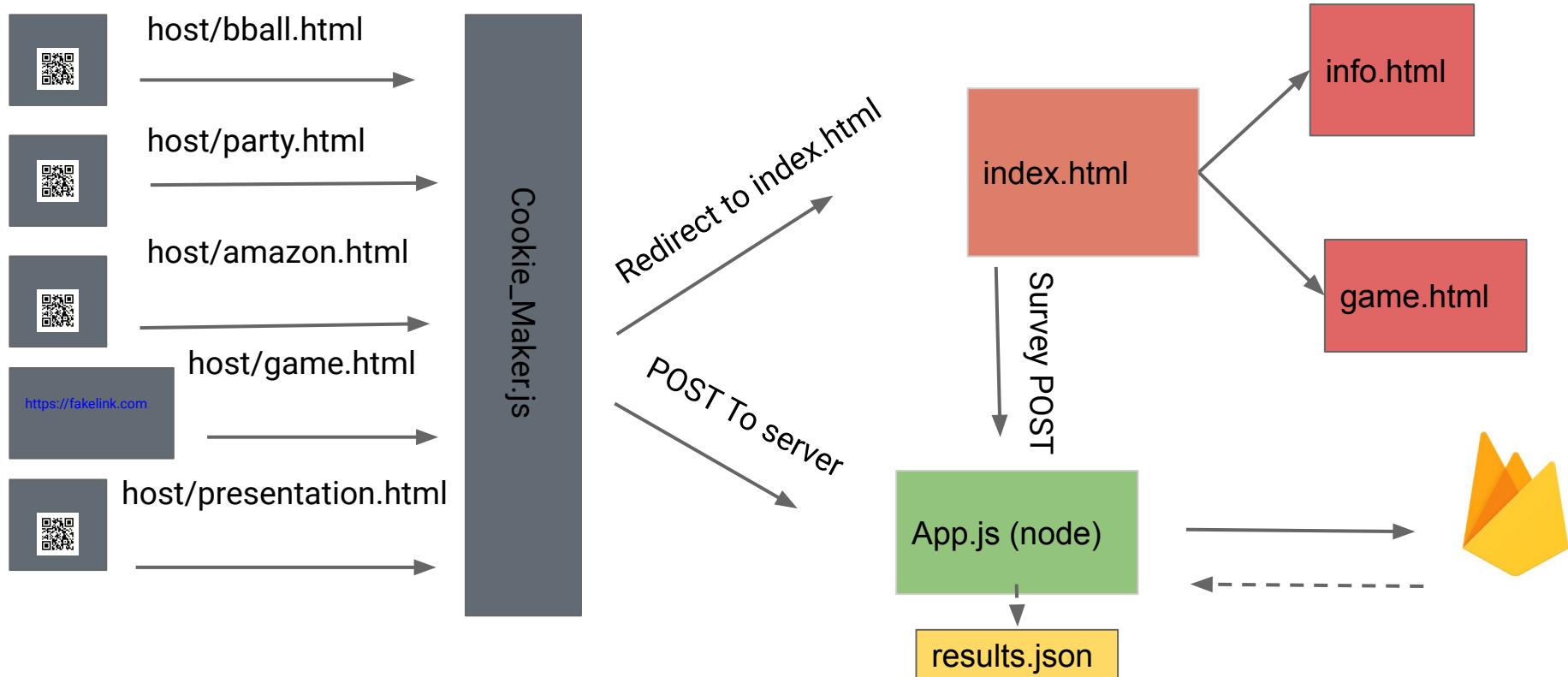
Click below to read more about the problem

<https://www.washingtonpost.com/technology/2011/10/07/ars-qr-codes-safe/>

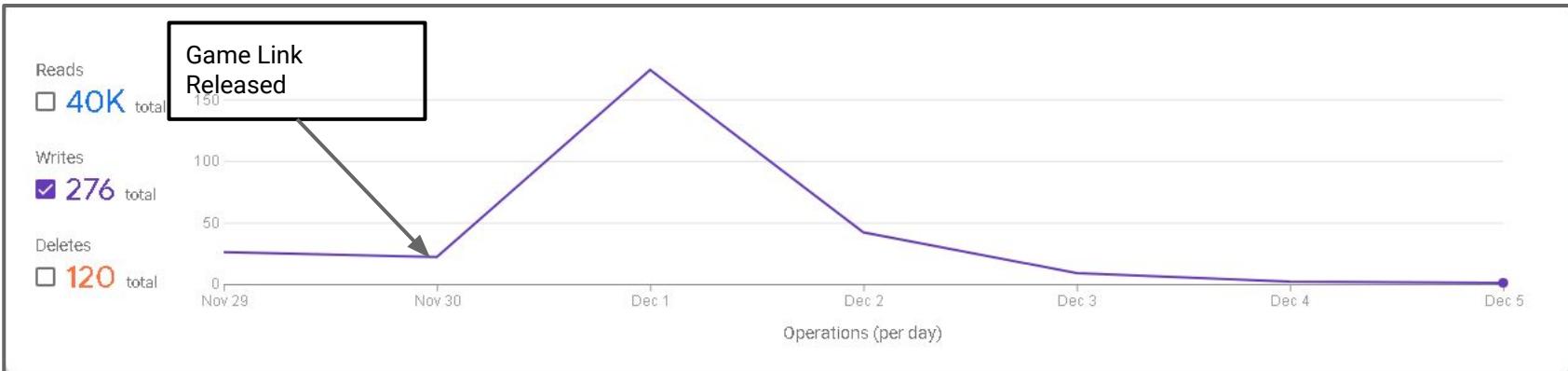
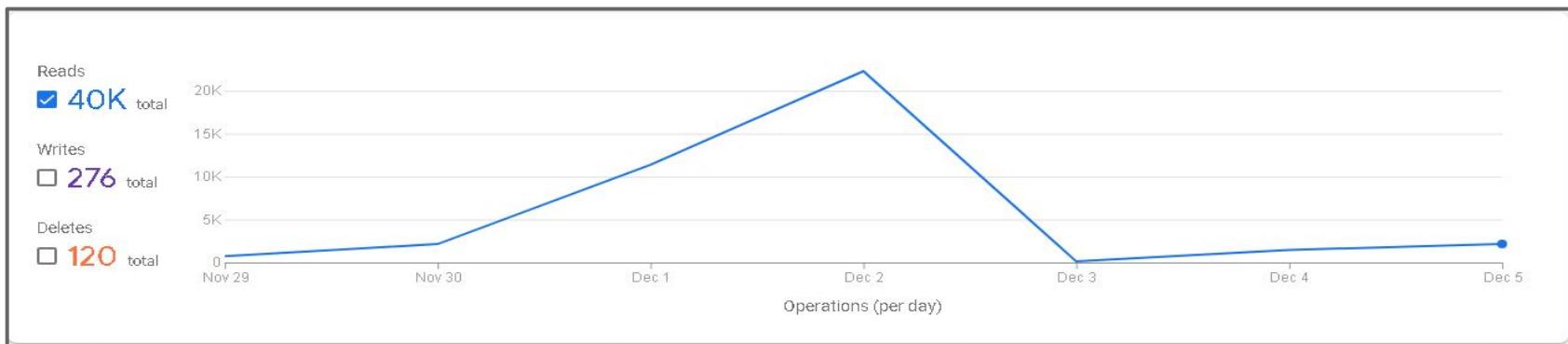
play the game (if you're on a computer)



How it worked



Our Experiment: FireStore DataBase



FireStore Continued...

The screenshot shows the Google Cloud Firestore interface. On the left, there's a sidebar with a project named "ec521project" and a "clientInfo" collection. Inside the "clientInfo" collection, there are several documents, one of which is selected and expanded. The selected document is named "YDF4Vo4YR7QnWMiX2hqo". This document contains the following fields:

- Cookies: "1491892687.1638153312"
- IP: "168.122.210.121"
- Source: "Amazon QRCode"
- Time: "2021-11-29T13:11:05.367Z"
- User: "Mozilla/5.0 (Linux; Android 10; SAMSUNG SM-G960U) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/16.0 Chrome/92.0.4515.166 Mobile Safari/537.36"

Our Experiment: Game Link



President Brown Game Available Now!

Post is awaiting moderator approval.
This post is currently awaiting approval by the moderators of [r/BostonU](#) before it can appear in the subreddit.

2 Comments Share Save Hide Report 38% Upvoted

Log in or sign up to leave a comment Log In Sign Up

Sort By: Best

dandillofficial · 5 days ago · edited 5 days ago
Titan of Chemistry

Clicked the link and it immediately installed malware on my computer, accessed all of my stored passwords, wired all of my money to Chinese scammers, stole my League of Legends account, and killed my dog. 9/10, the UI could use some updates and the endgame content starts to get a bit boring.

In all seriousness, I'm on mobile so I haven't clicked the link, but do be careful when clicking links sent by hour-old reddit accounts.

Edit: still on mobile but copying text from the post shows you exactly where the link leads:
https://salty-peak-17003.herokuapp.com/P3_G1.html

Obviously this isn't the same thing as "bugames.com", which isn't a real site. Don't click the link!

15 Reply Share Report Save

hyp-o-algesia · 5 days ago

Site literally breaks with my addons lmao

AND I live dangerously don't tell me what not to click!!!!!!

1 Reply Share Report Save

Survey Results

"rip my tuition"

"Did someone hack me"

"nice"

"Really interesting, when I saw this I pop up I was like
I've never really thought about that"

"False advertising bullshit"

"This is kind of a stupid experiment. Why would I
expect a phasing scam on a student Facebook group
with user authentication required to enter?"

"Okay Yes"

"I have client sided protection that would halt and alert
before anything was executed or downloaded."

"Hmm"

"Interesting"

"I love it!"

"Cool. Good way to see how dumb people are (clearly I
am lol)"

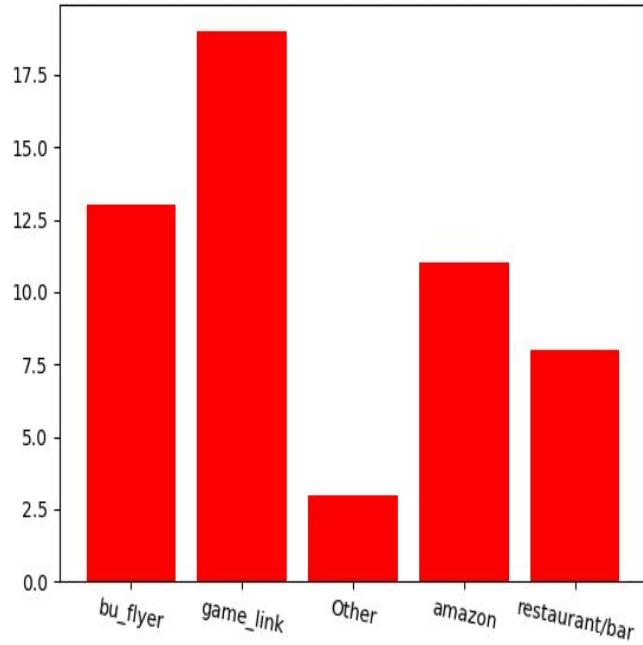
"Convincing"

"Yes"

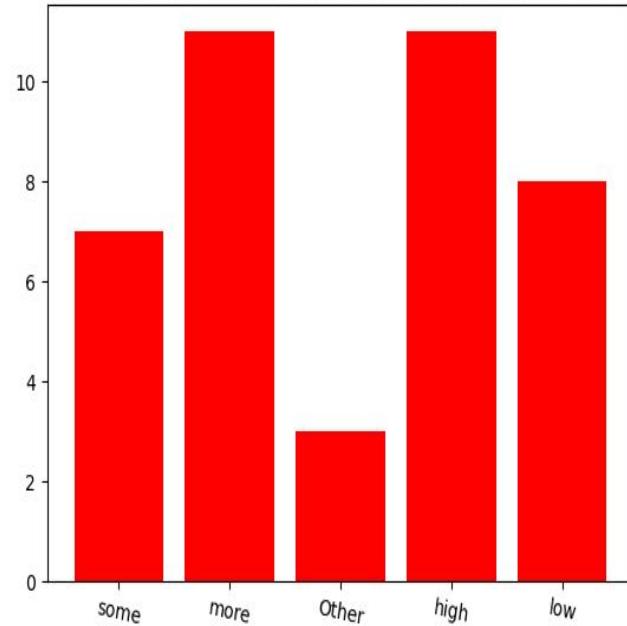
"this exp gave me a descent scare. its a good way of
spreading important information"

Results Continued

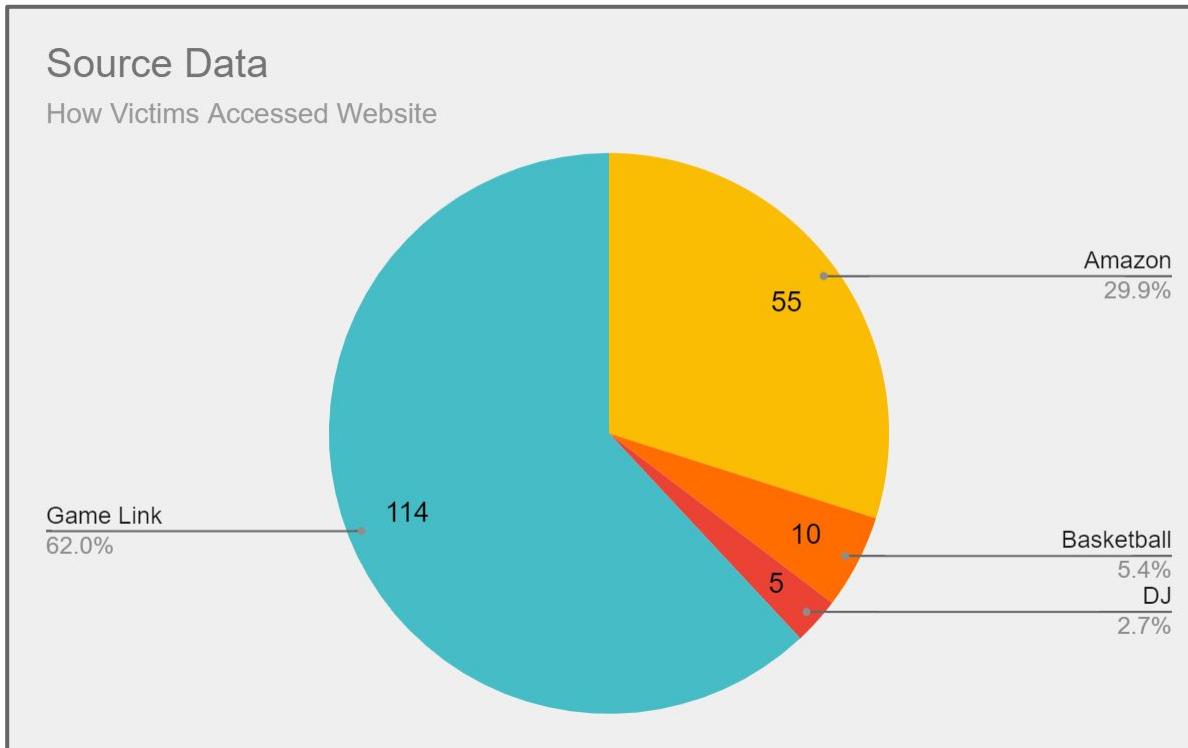
Histogram of Self Report Location (total):40



Histogram of Security Level (total):40

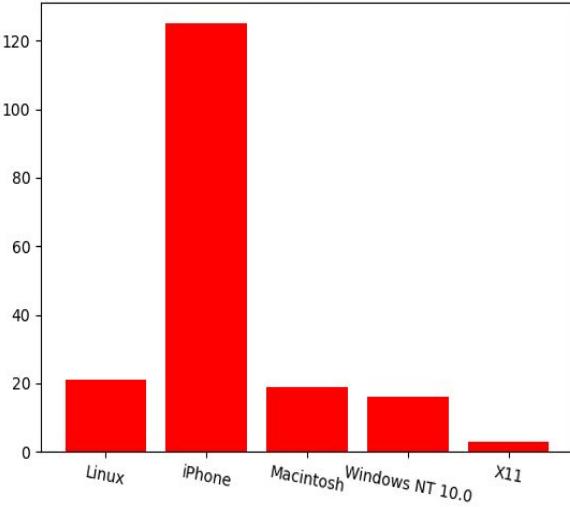


Results Continued



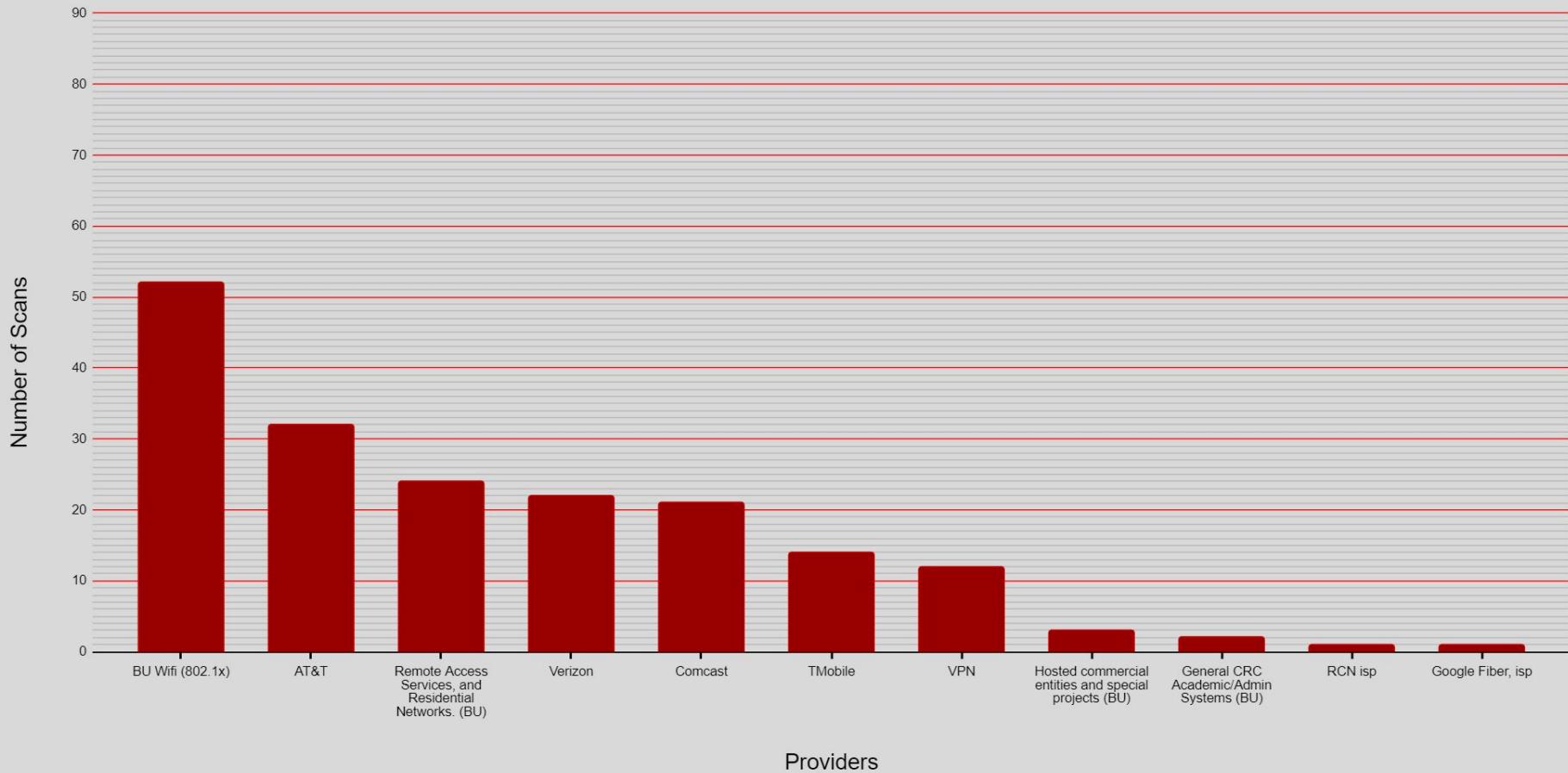
Results Continued

Histogram of Device



(Linux; Android 11; Pixel 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.4.606.85 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 14_B like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/18H107 [FBAN/FBOS;FBDV/Phone13;FBMD/Phone;FBSN/OS;FBSV/14.8;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Linux; Android 12; SM-G991U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1"
(Linux; Android 11; SAMSUNG SM-G991U) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/15.0 Chrome/90.0.4430.210 Mobile Safari/537.36"
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19A346 [FBAN/FBOS;FBDV/Phone11;FBMD/Phone;FBSN/OS;FBSV/15.0;FBSS/2;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 15_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B81 [FBAN/FBOS;FBDV/Phone14.5;FBMD/Phone;FBSN/OS;FBSV/15.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 14_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 14_5_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.1 Mobile/15E148 Safari/604.1"
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.15 (KHTML, like Gecko) Version/14.1.2 Safari/605.1.15"
(X11; CrOS x86_64 13982.88_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.162 Safari/537.36"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/18H107 [FBAN/FBOS;FBDV/Phone11;FBMD/Phone;FBSN/OS;FBSV/14.8;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B74 [FBAN/FBOS;FBDV/Phone12;FBMD/Phone;FBSN/OS;FBSV/15.1;FBSS/2;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/18H17 [FBAN/FBOS;FBDV/Phone13;FBMD/Phone;FBSN/OS;FBSV/14.8;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Linux; Android 12; Pixel 5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 15_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"
(Linux; Android 11; SM-G973U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"
(Linux; Android 10; Nokia 7 plus Build/QKQI_190820_002; w) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4664.45 Mobile Safari/537.36"
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B81 [FBAN/FBOS;FBDV/Phone14.5;FBMD/Phone;FBSN/OS;FBSV/15.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"
(Linux; Android 11; SM-G991U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Linux; Android 12; Pixel 4 (G) Build/SPIA_211105_003; w) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4664.45 Mobile Safari/537.36"
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Version/15.1 Safari/605.1.15"
(Linux; Android 12; Pixel 5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"
(Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Safari/537.36"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Linux; Android 11; SM-G973U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 14_B_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"
(Linux; Android 12; Pixel 4 (G) Build/SPIA_211105_003; w) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4664.45 Mobile Safari/537.36"
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Version/15.1 Safari/605.1.15"
(Linux; Android 12; Pixel 5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Mobile Safari/537.36"
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1"

IP Address Data



Why Our Data Is Important

- We've shown that even over a short period of time, dozens upon dozens of people unknowingly gave us information.
- More sophisticated attacks could easily get more private data, and abuse other web-based attacks, and we are increasing awareness of that.
- Digital security awareness is vital to bridging the digital divide and allowing everyone to properly and safely use the internet.
- The varied flyers and various carriers show that there is not one demographic that is more at risk, and that cybersecurity education is very important.

Our Solution

YSSQCYDT (You Shouldn't Scan QR Codes You Don't Trust)

Also you shouldn't click on all links that you see.

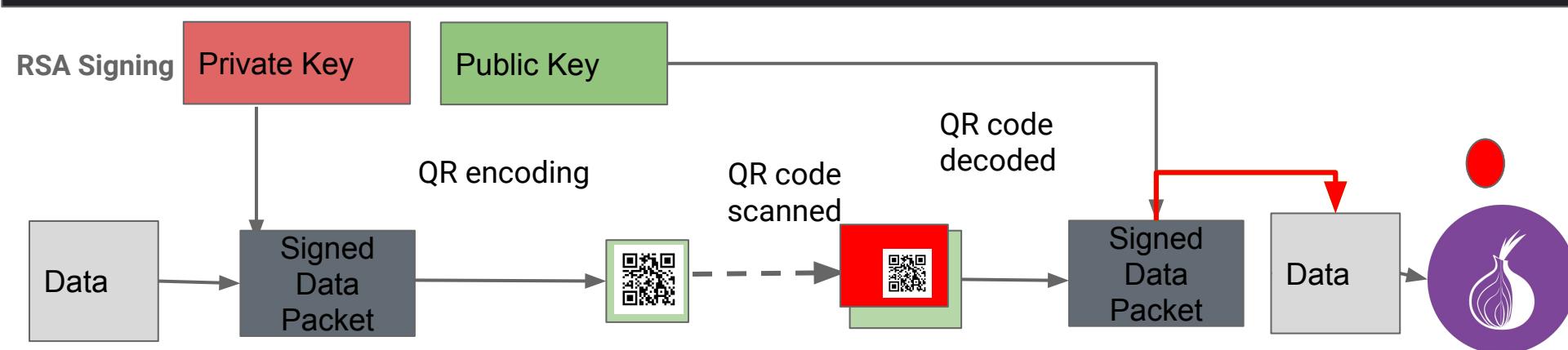
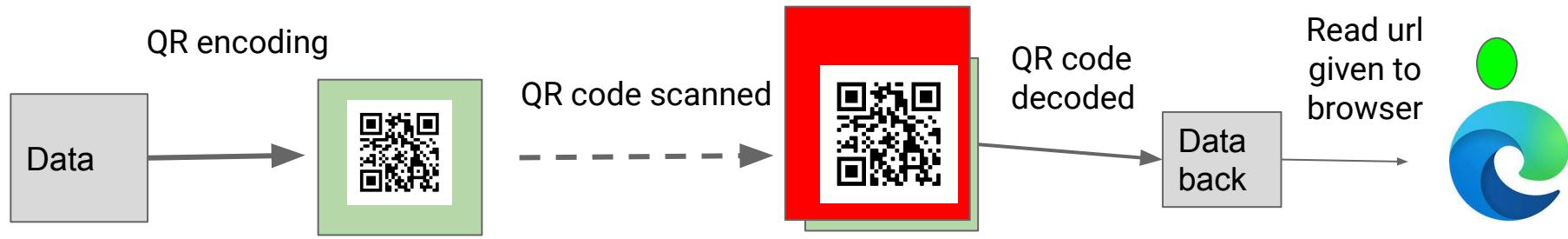
QR codes are a media for storing arbitrary information

They contain no security at all.

Scanning them blindly may leave you vulnerable to:

- Malicious Javascript
- Malware downloads
- BotNets(an attack that uses your computer or phone for its processing power, i.e. to mine bitcoin)
- Man-in-the-middle attacks(an attack where the attacker pretends to be the website you expected and steals your inputs and the websites outputs)
- Cross site scripting attacks (an attack that allows websites to steal your cookies)
- Phishing scams
- Cross site Request forgery(an attack that uses your cookies to gain access to a different site you are authenticated to.)
- Arbitrary code execution
- And Many more

Our Solution Continued...



Thank You

We will now open up the floor to
any questions