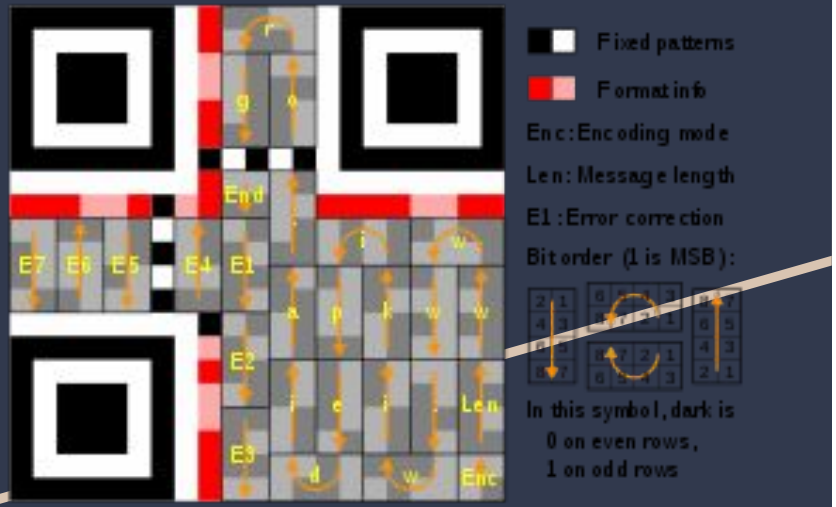
Quick Response (QR) Code Security

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 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

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? Other
What is your level of technical understanding? NA
(optional)Thoughts on the experiment?
Submit

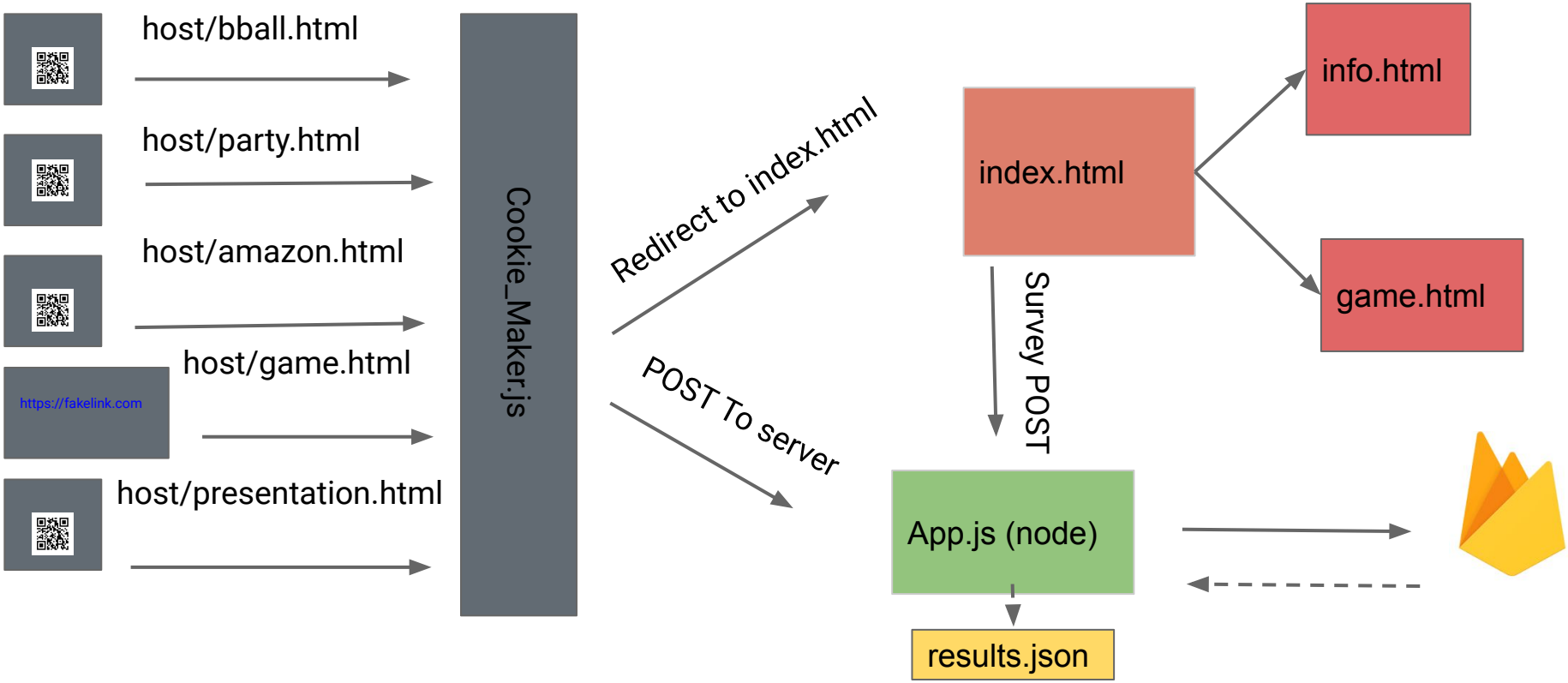
Click below to read more about the problem

https://www.washingtonpost.com/technology/2021/10/07/are-qr-codes-safe/

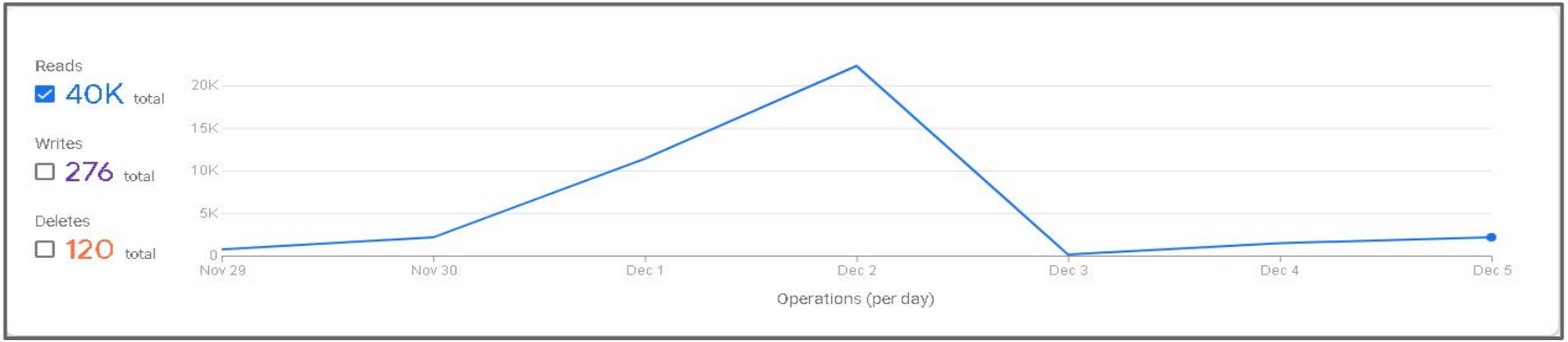
play the game (if your on a computer)

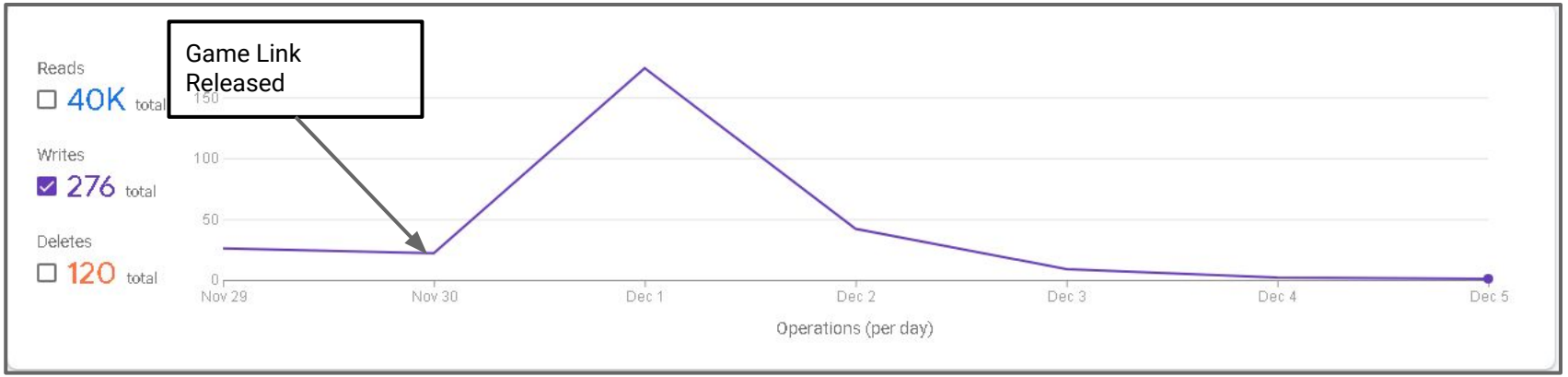
This website was created as part of a research project for BU EC 521. For any questions or concerns please contact tottto45@gmail.com

How it worked



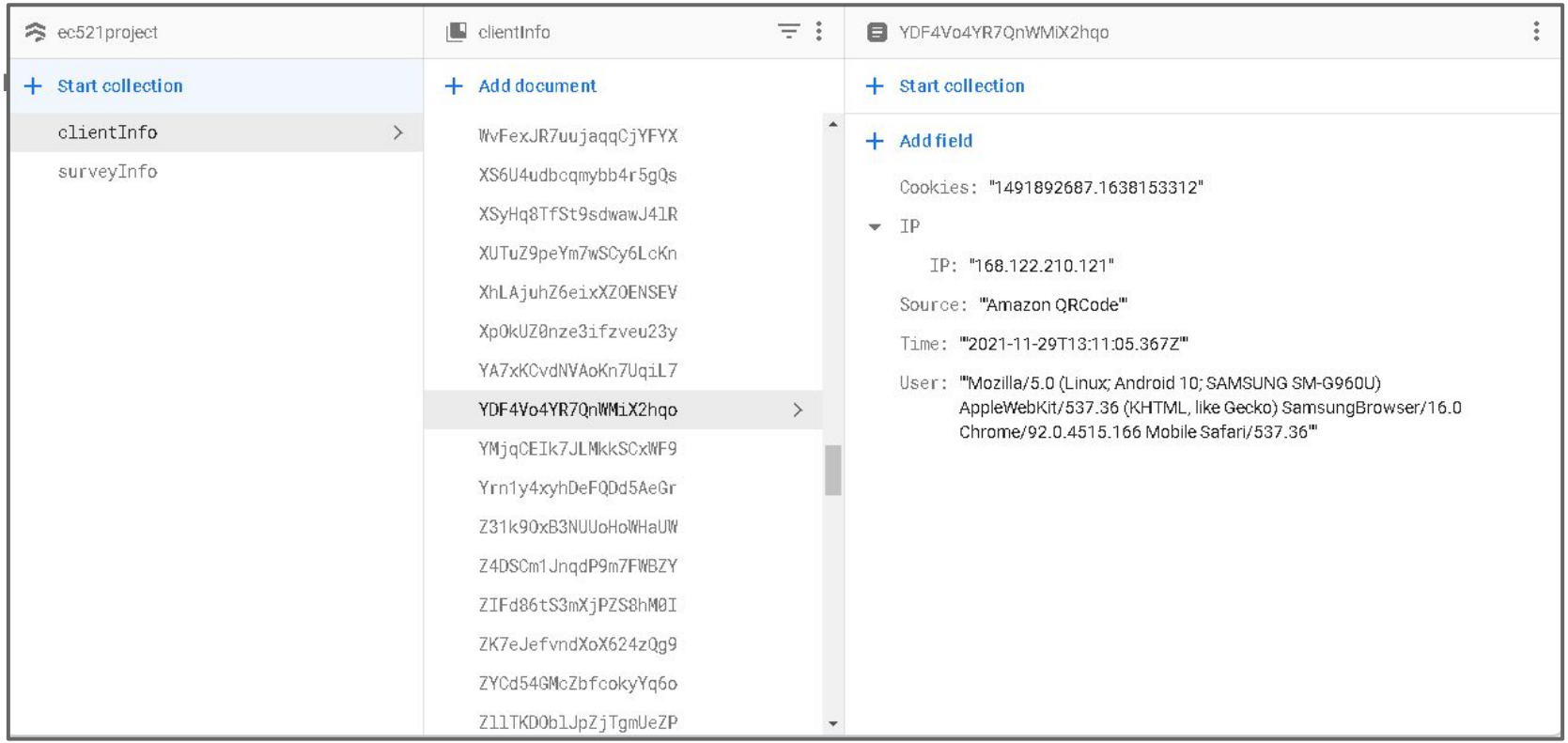
Our Experiment: FireStore DataBase



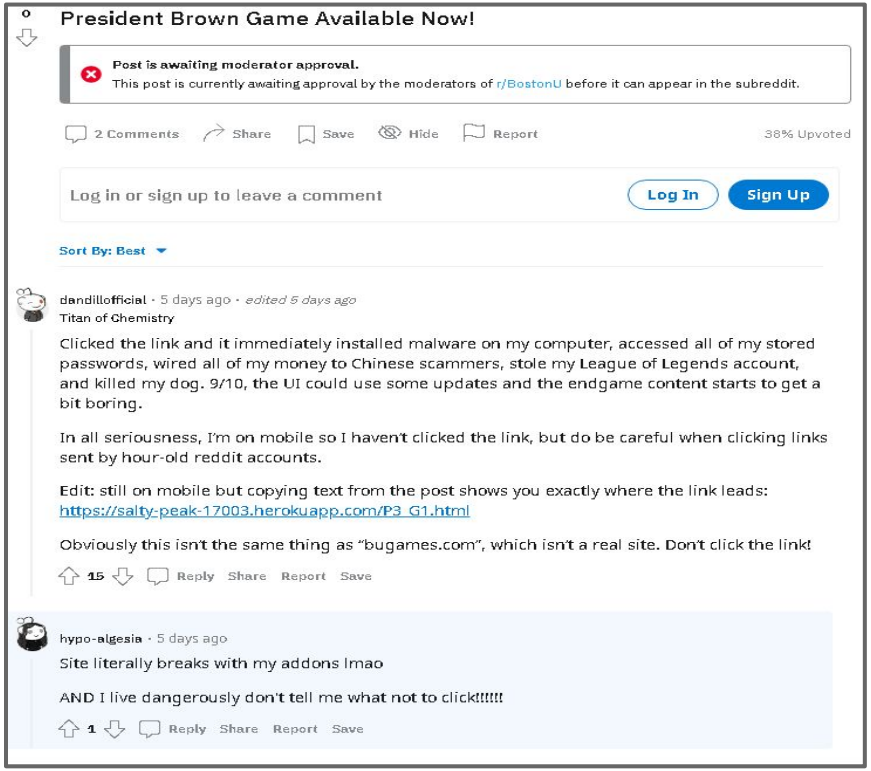


FireStore Continued...

Gar



Our Experiment: Game Link



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!"

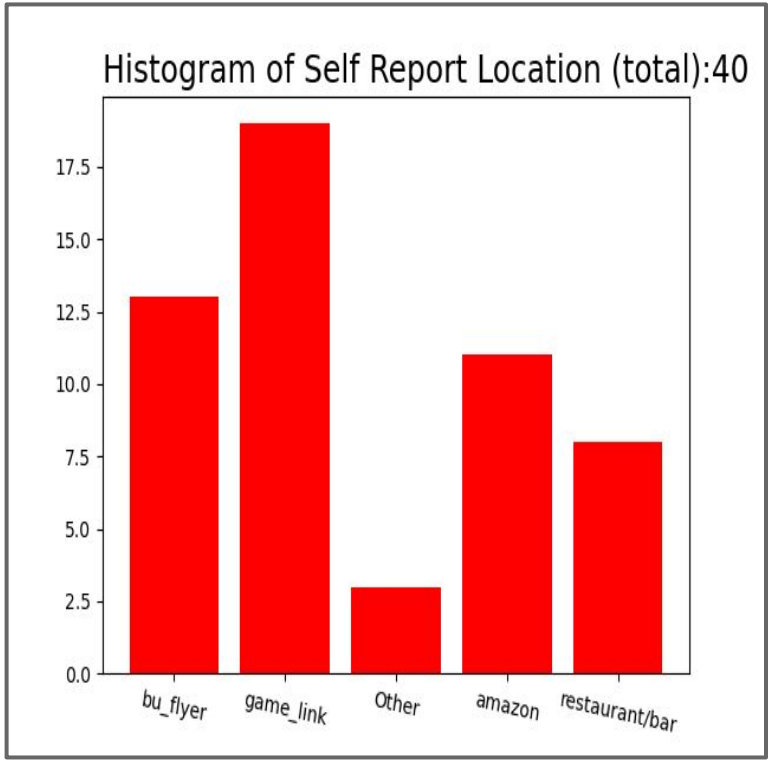
"Cool. Good way to see how dumb people are (clearly I am lol)"

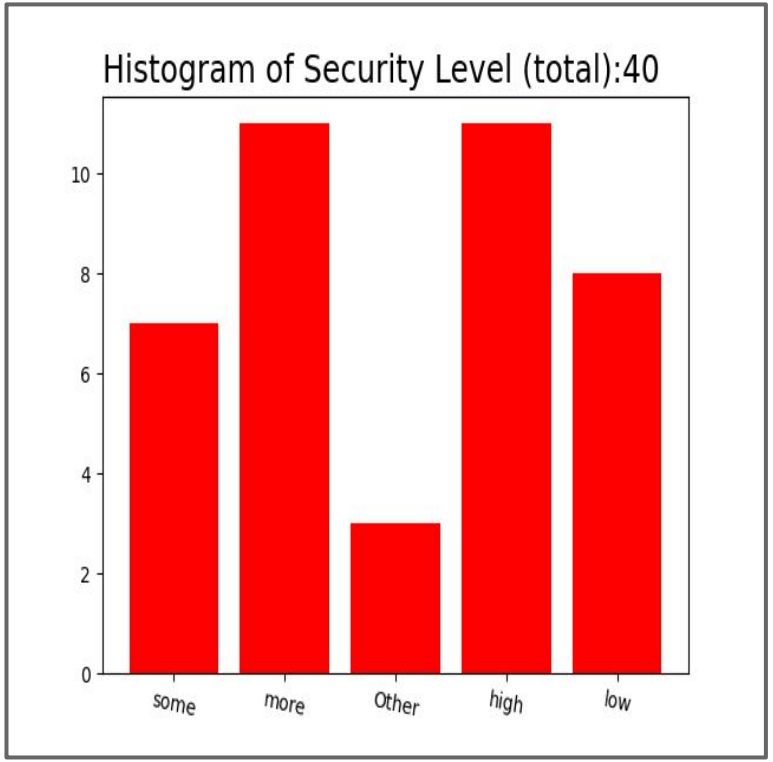
"Convincing"

"Yes"

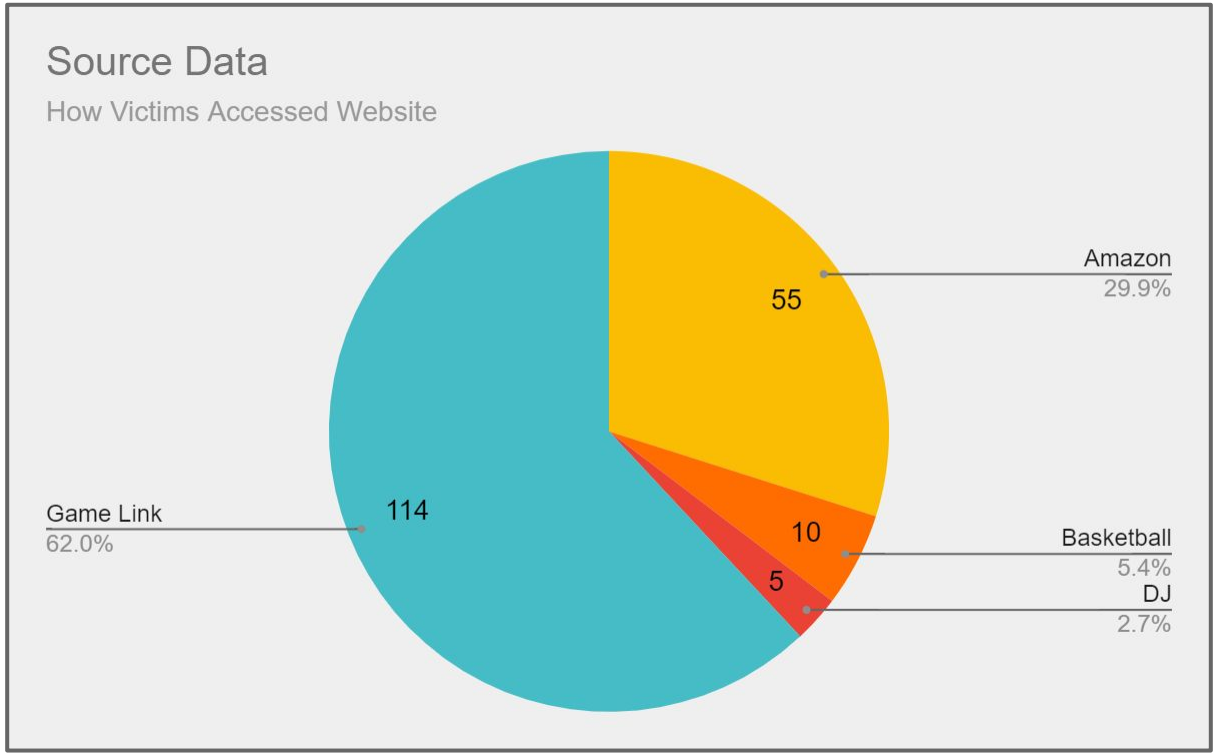
"this exp gave me a descent scare. its a good way of spreading important information"

Results Continued

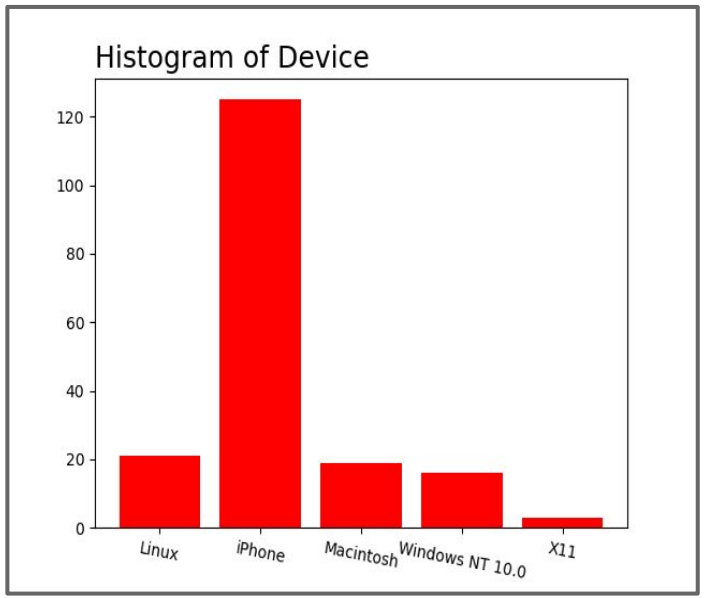




Results Continued

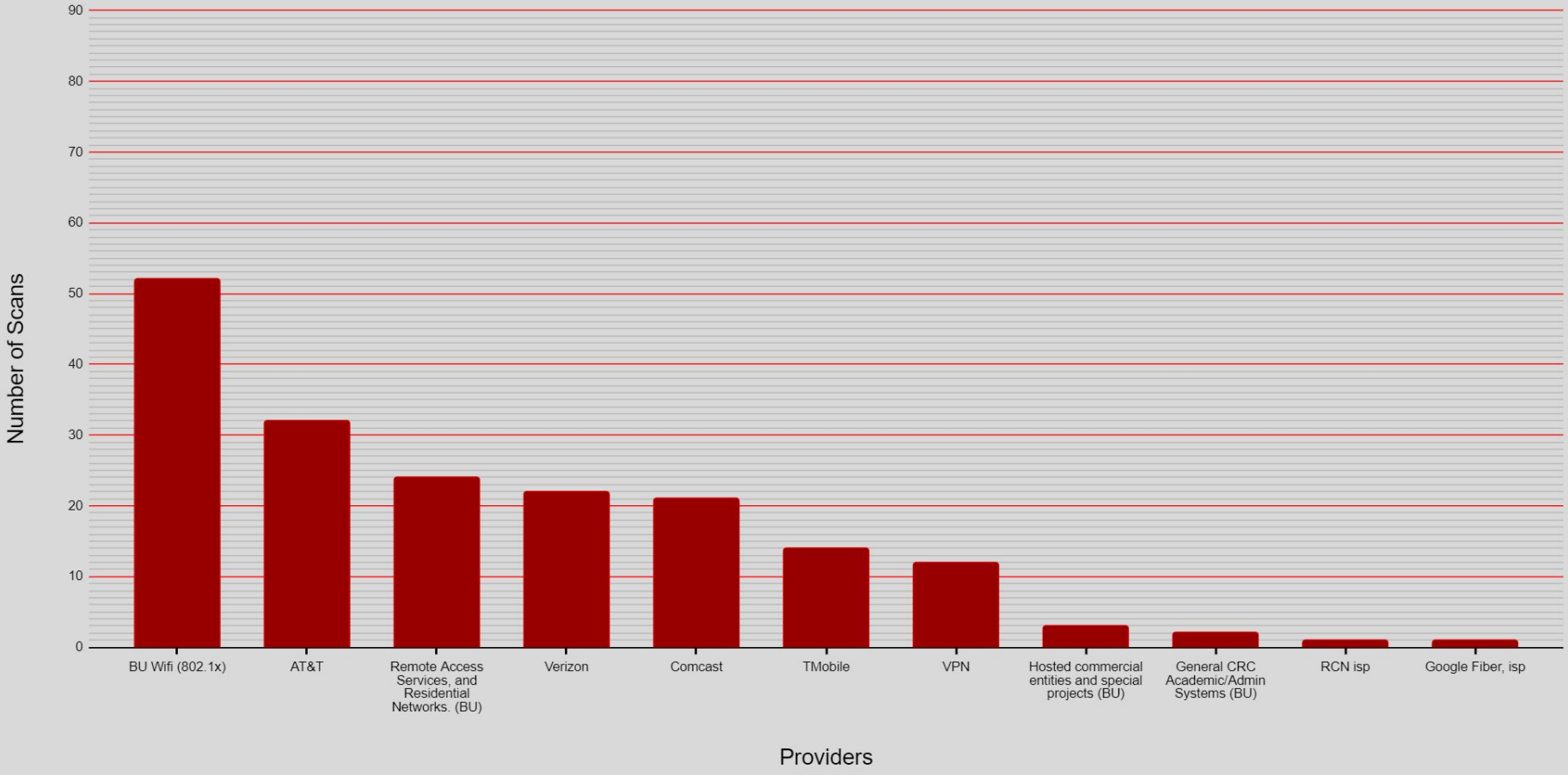


Results Continued



(Linux; Android 11; Pixel 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.85 Mobile Safari/537.36"	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"	1
(iPhone; CPU iPhone OS 14_8 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"	1
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/18H107 [FBAN/FBIOS;FBDV/iPhone13,3;FBMD/iPhone;FBSN/iOS;FBSV/14.8.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"	9
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1
(Linux; Android 12; SM-G991U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"	1
(iPhone; CPU iPhone OS 15_0_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1"	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"	1
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"	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"	1
(iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19A346 [FBAN/FBIOS;FBDV/iPhone11,8;FBMD/iPhone;FBSN/iOS;FBSV/15.0;FBSS/2;FBID/phone;FBLC/en_US;FBOP/5]"	1
(iPhone; CPU iPhone OS 15_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B81 [FBAN/FBIOS;FBDV/iPhone14,5;FBMD/iPhone;FBSN/iOS;FBSV/15.1.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"	1
(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"	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"	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"	1
(iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.1 Mobile/15E148 Safari/604.1"	1
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Safari/605.1.15"	1
(X11; CrOS x86_64 13982.88.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.162 Safari/537.36"	2
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/18H107 [FBAN/FBIOS;FBDV/iPhone11,2;FBMD/iPhone;FBSN/iOS;FBSV/14.8.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"	7
(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"	1
(iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B74 [FBAN/FBIOS;FBDV/iPhone12,8;FBMD/iPhone;FBSN/iOS;FBSV/15.1;FBSS/2;FBID/phone;FBLC/en_US;FBOP/5]"	1
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	9
(iPhone; CPU iPhone OS 14_8 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/18H17 [FBAN/FBIOS;FBDV/iPhone13,4;FBMD/iPhone;FBSN/iOS;FBSV/14.8;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"	1
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1
(Linux; Android 12; Pixel 5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"	1
(iPhone; CPU iPhone OS 15_0_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1"	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"	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"	1
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"	1
(Linux; Android 11; SM-G973U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"	1
(Linux; Android 10; Nokia 7 plus Build/QKQ1.190828.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4664.45 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/345.0.0.34.118;]"	6
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"	1
(iPhone; CPU iPhone OS 15_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19B81 [FBAN/FBIOS;FBDV/iPhone14,5;FBMD/iPhone;FBSN/iOS;FBSV/15.1.1;FBSS/3;FBID/phone;FBLC/en_US;FBOP/5]"	1
(Linux; Android 11; SM-G991U1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Mobile Safari/537.36"	1
(iPhone; CPU iPhone OS 14_7_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1
(Linux; Android 12; Pixel 4a (5G) Build/SP1A.211105.003; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4664.45 Mobile Safari/537.36"	1
(Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Safari/605.1.15"	1
(Linux; Android 12; Pixel 5a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Mobile Safari/537.36 EdgA/96.0.1054.36"	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"	2
(Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Safari/537.36"	1
(iPhone; CPU iPhone OS 14_8_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1"	1

IP Address Data

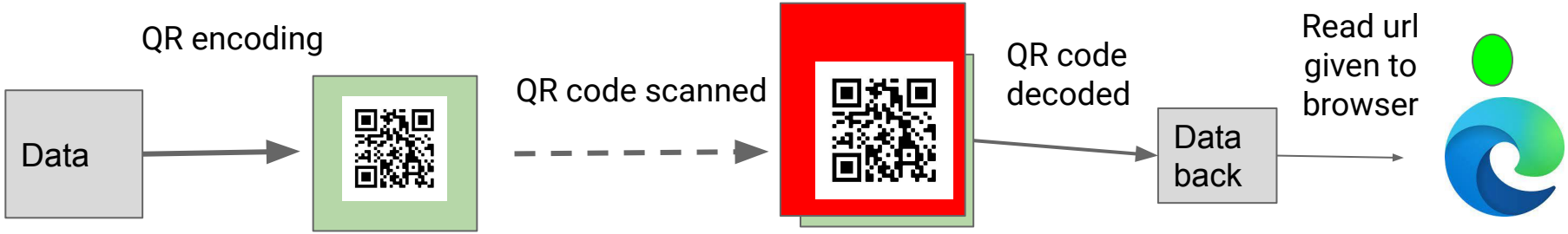


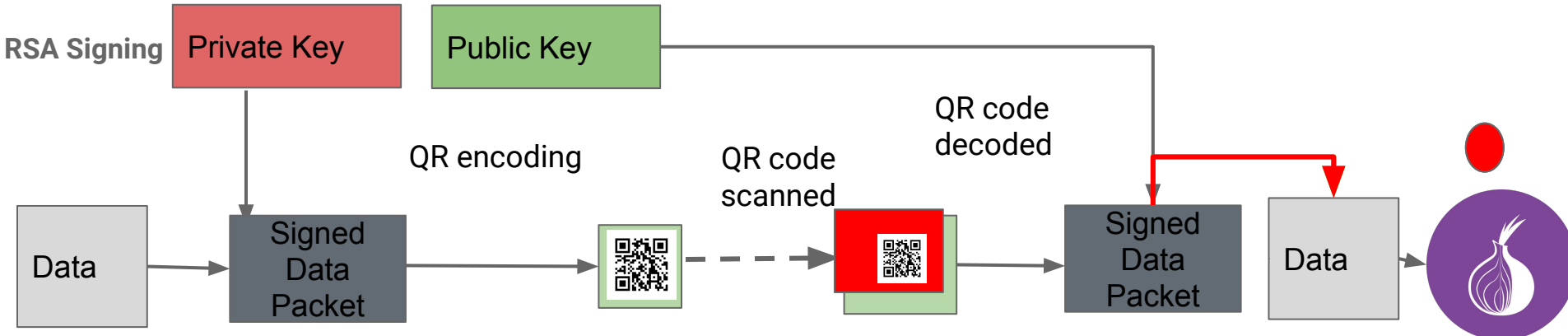
Why Our Data Is Important

- 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

Our Solution Continued...





Thank You

We will now open up the floor to any questions