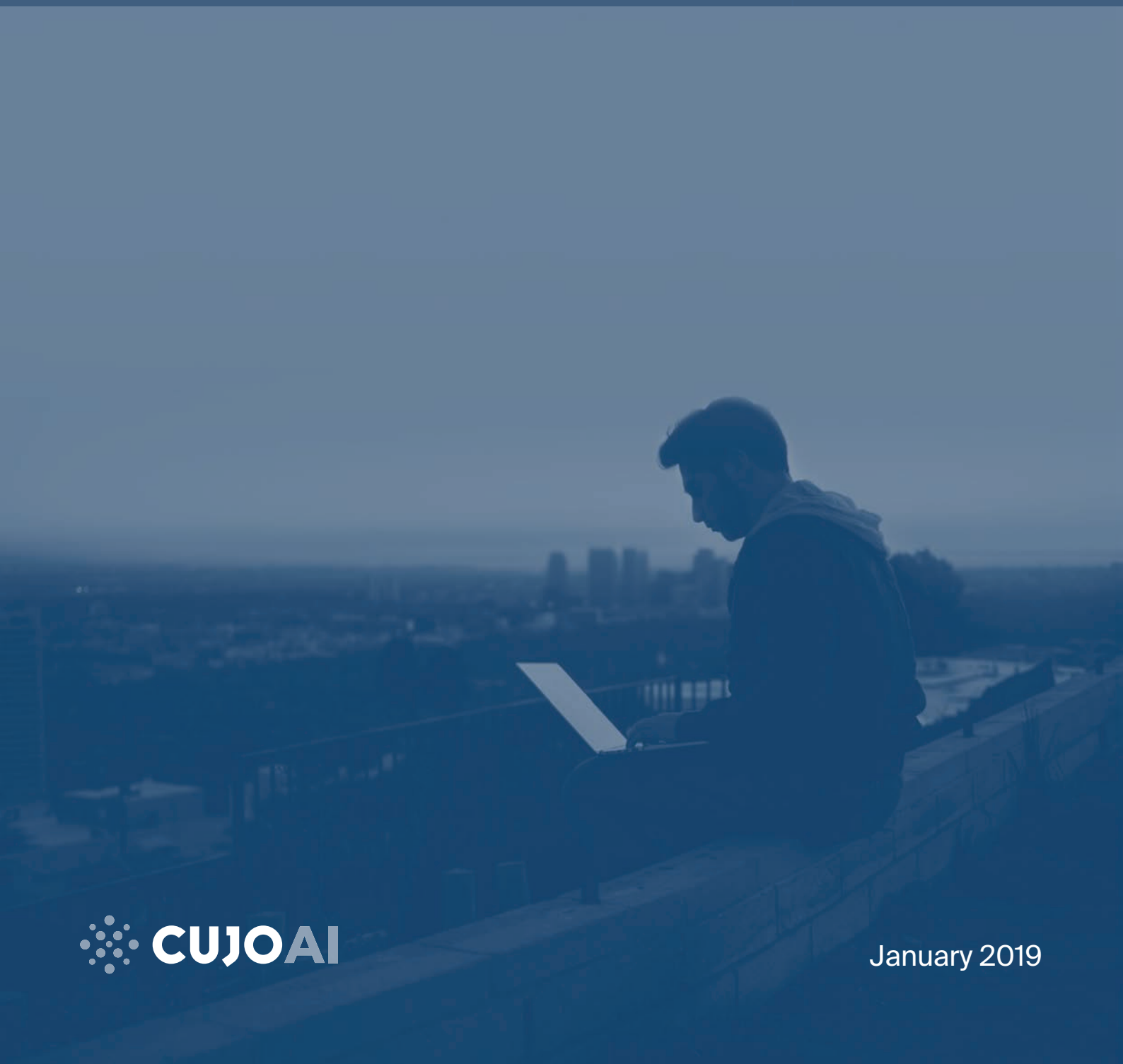
Cybersecurity Perceptions

The connected experience from the end-user perspective



CUJOAI

January 2019

Table of Contents

Overview

In 2018, a typical American home had 13-14 smart devices. The number includes not only smartphones and laptops but also wearables and other IoT devices.

While connected devices continue to populate homes, they are being targeted by emerging new attack methods. Cybercriminals seek to take advantage of unprotected home networks, and most of the end users are aware of the new threats. However, they lack knowledge or appropriate tools to address this shift in home security.

This report presents end-user cybersecurity perceptions about their connected experience and their take on cybercrime prevention.

CUJO AI Cybersecurity Perception Survey

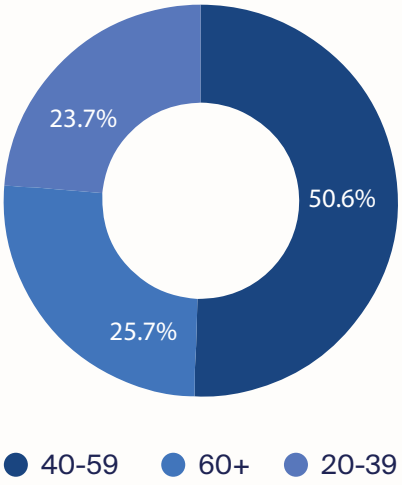
In December 2018, we have conducted a semi-structured online survey to analyze end-user perceptions about cybersecurity. This survey contains responses from 2034 owners of CUJO AI Internet Security Firewall in the U.S.

CUJO AI Threat Intelligence Database

In this report, we have used aggregated anonymized behavioral data from a randomized sample of 1M devices that were connected in the U.S. households. The analysis was carried out using data from 2018 Q4.

Demographics

Most of the people surveyed are early adopters who have been living in a smart home for months. They are past the novelty phase and into day-to-day use of multiple smart devices with the averages ranging from 13 to 14 devices per household at the given period.



Age

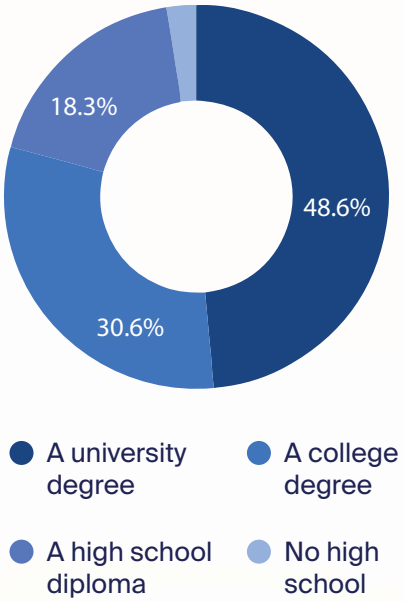
The majority of respondents are Generation X or baby boomers.

According to United States Department of Labour data, baby boomers and generation X have the highest expenditure share compared with other generations.[1]

Education

The majority of survey participants are well educated: 79.2% have a college or a university degree.

They believe they have sufficient knowledge about cybersecurity. 59.1% of respondents feel well informed about cyber threats.



[1] *Shares of annual aggregate expenditures and sources of income, Consumer Expenditure Survey [2017], United States Department of Labour, https://www.bls.gov/cex/[2017]/aggregate/gener.pdf*

Key Findings

The end-user perception survey has revealed that early adopters are aware of the cyber threats. However, in the past 12 months, they've been mostly using the traditional cybersecurity tools to protect themselves against cybercriminals.

Even having considerable knowledge, survey participants do not believe that they can protect themselves against the threats. More than two-thirds are not sure if they can identify when their device is under attack.

The majority of survey participants conclude that cybersecurity should be a combined effort between end-users, governments, ISPs, and other stakeholders.

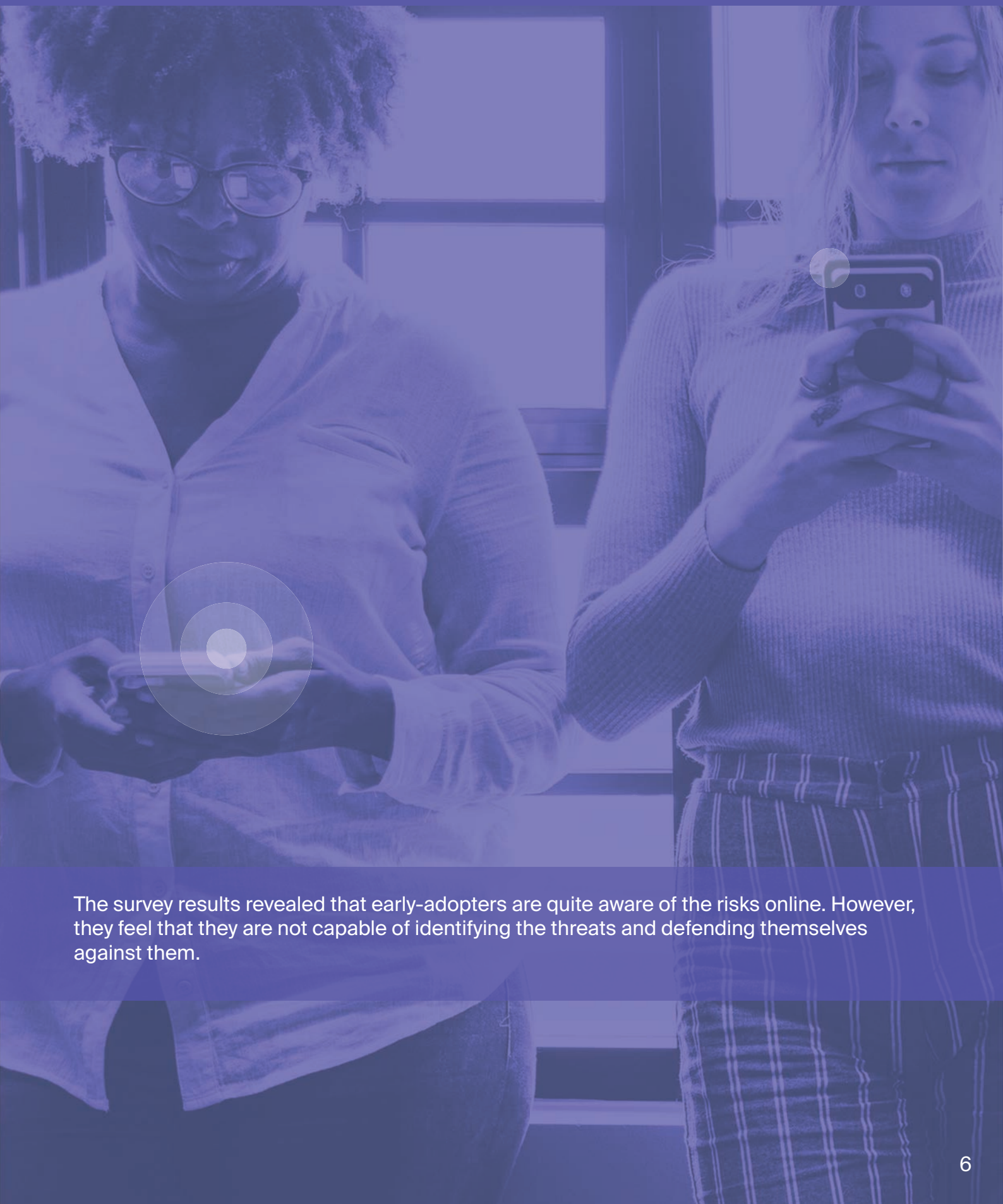
End-user perceptions about cybersecurity:

- The majority of survey participants (89.6%) are well aware of increasing cyber risks
- Less than half (48.8%) of respondents think that they can protect themselves from cyber threats
- 61.2% of respondents are not sure or claim that they cannot identify if their device is under attack

The Current State of Prevention and Protection:

- Survey participants fail to identify smart home devices that are the most vulnerable
- Respondents still rely on traditional security means (i.e., improving their passwords or installing antivirus)
- Respondents are not sure who is responsible for their protection but think that cybercrime prevention should be a combined effort (85.2%)

Perception of Cybersecurity

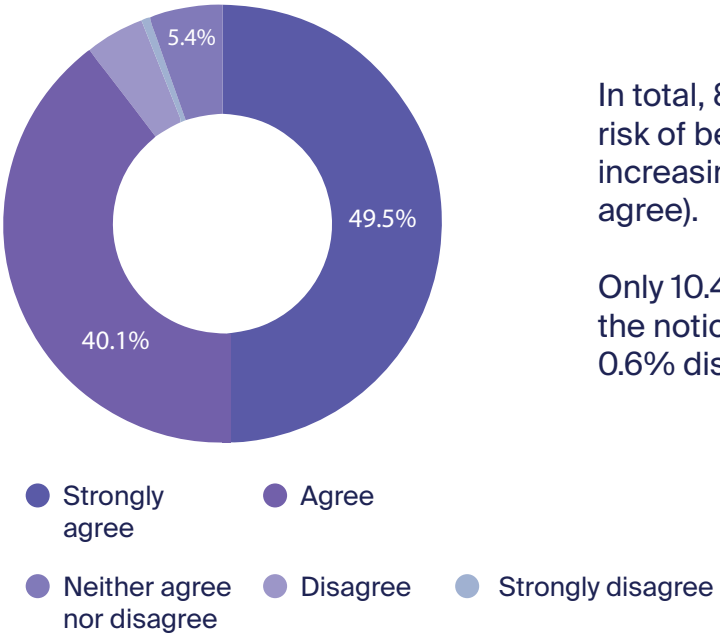


The survey results revealed that early-adopters are quite aware of the risks online. However, they feel that they are not capable of identifying the threats and defending themselves against them.

Awareness

Survey participants consider themselves to be aware of the increasing cyber risks.

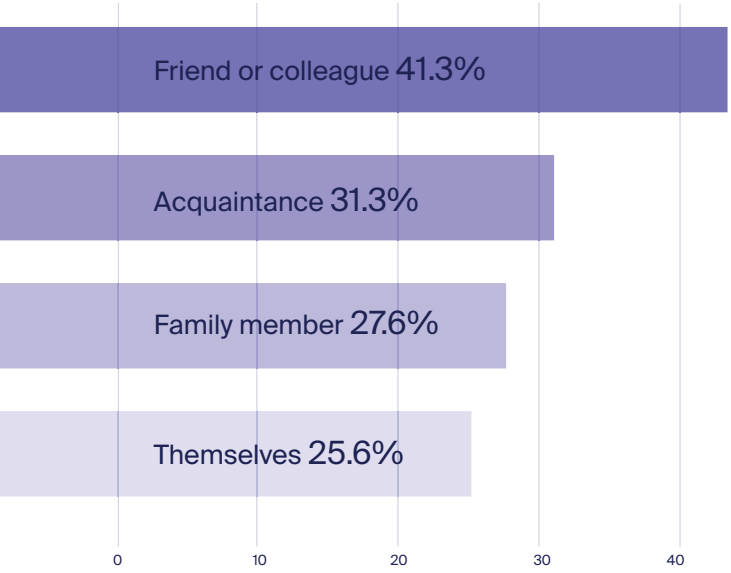
Do you agree or disagree with the following statements? “I believe that the risk of becoming a victim of cybercrime is increasing”



In total, 89.6% of respondents think that the risk of becoming a victim of cybercrime is increasing (40.1% agree & 49.5% strongly agree).

Only 10.4% are not sure or don’t agree with the notion (4.4% neither agree nor disagree, 0.6% disagree & 5.4% strongly disagree).

Have you or people you know been a victim of cybercrime?



When asked if they know anyone who was a victim of cybercrime, 41.3% chose their friend or colleague, 31.3% listed their acquaintance, and 27.6% selected a family member.

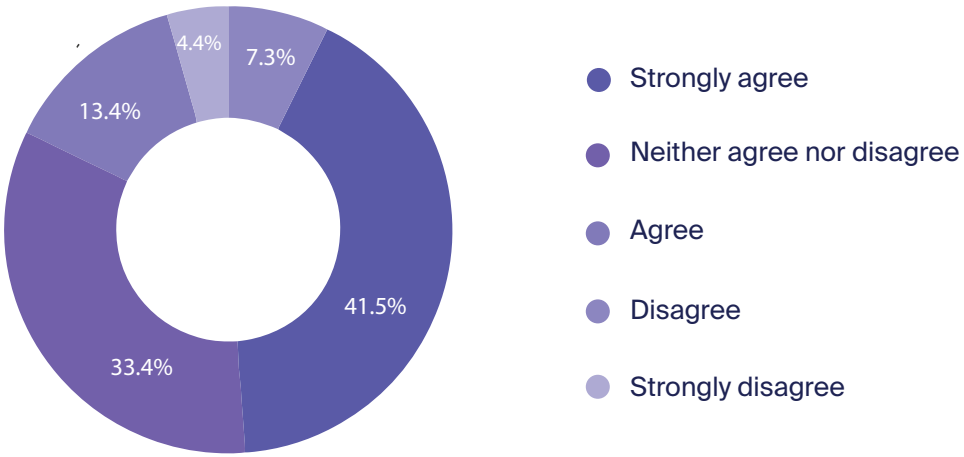
25.6% of respondents claim that they have been a victim of cybercrime themselves.

Confidence

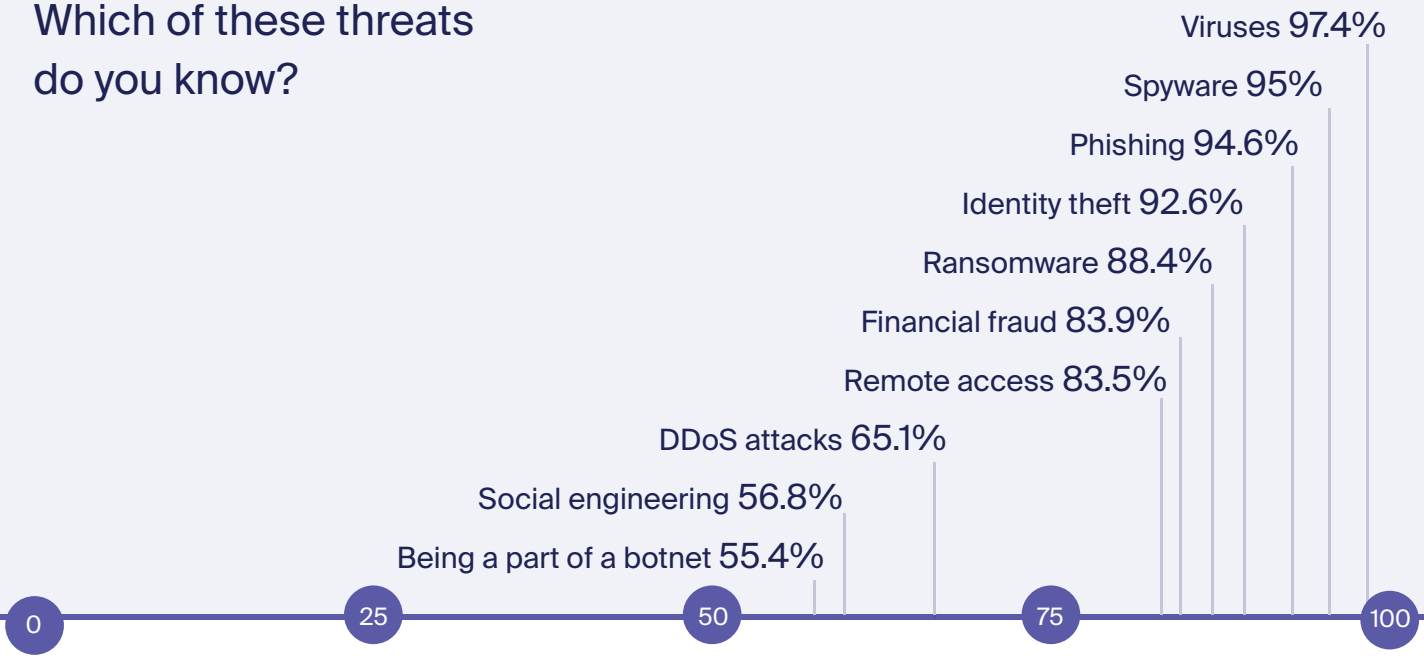
More than half of survey participants are not sure if they can protect themselves against cyber threats.

51.2% of respondents are not sure or don't think that they can protect themselves from cyber threats. 41.5% agree & 7.3% strongly agree that they can protect themselves.

Do you agree or disagree with the following statements? "I think that I am able to protect myself from cyber threats"



Which of these threats do you know?



The survey participants are aware of most of the common threats. They can identify different types of malware (viruses, spyware, ransomware), know about phishing, are aware of identity theft and financial fraud.

Cybersecurity Landscape

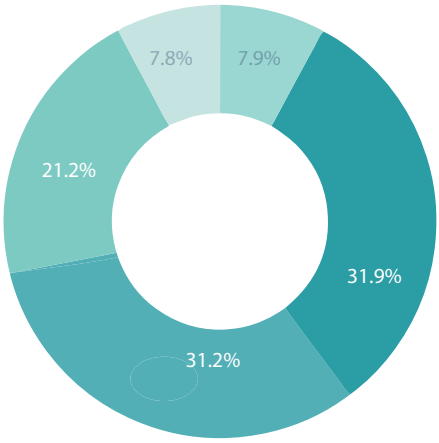
Survey participants have trouble identifying when their device is under attack or pointing out vulnerable devices in general. They tend to implement traditional cybersecurity methods. Most of the people surveyed think that cybercrime should be a combined effort between governments, companies, internet service providers, and the end-user.

Vulnerable Devices

More than two-thirds of the respondents do not think that they can identify if their devices are under attack.

61.2% of respondents are not sure or claim that they can't identify if their device is under attack. 39.8% feel confident that they are able to identify if their device is under attack (31.9% agree & 7.9% strongly agree)

Do you agree or disagree with the following statements? "I can identify if my device is under a cyber attack"



- Strongly agree
- Neither agree nor disagree
- Agree
- Disagree
- Strongly disagree

Which of these smart home devices are most vulnerable to cyber threats?

User Perception
The most vulnerable devices

1. Computer (PC, laptop, tablet) 83.9%
2. Router 72.9%
3. Smart TV 58.2%
4. Phone 56.2%
5. Camera 54.4%
6. Streaming devices 47.5%
7. Printer 42.2%
8. Thermostat 40.2%
9. Game console 36.9%
10. Doorbell 36.4%

CUJO AI Cybersecurity Perception Survey, 2018

Threat Intelligence Data
Devices that receive the most attacks

1. Computer (PC, laptop, tablet)
2. Phone
3. NAS storage
4. IP camera
5. Streaming video device
6. DVR
7. Access point
8. Wireless audio
9. Server
10. Router

CUJO AI Threat Intelligence Database, 2018 Q4

In the survey, participants highlighted the devices they think are the most vulnerable. CUJO AI researchers compared their perception with the CUJO AI threat intelligence database.

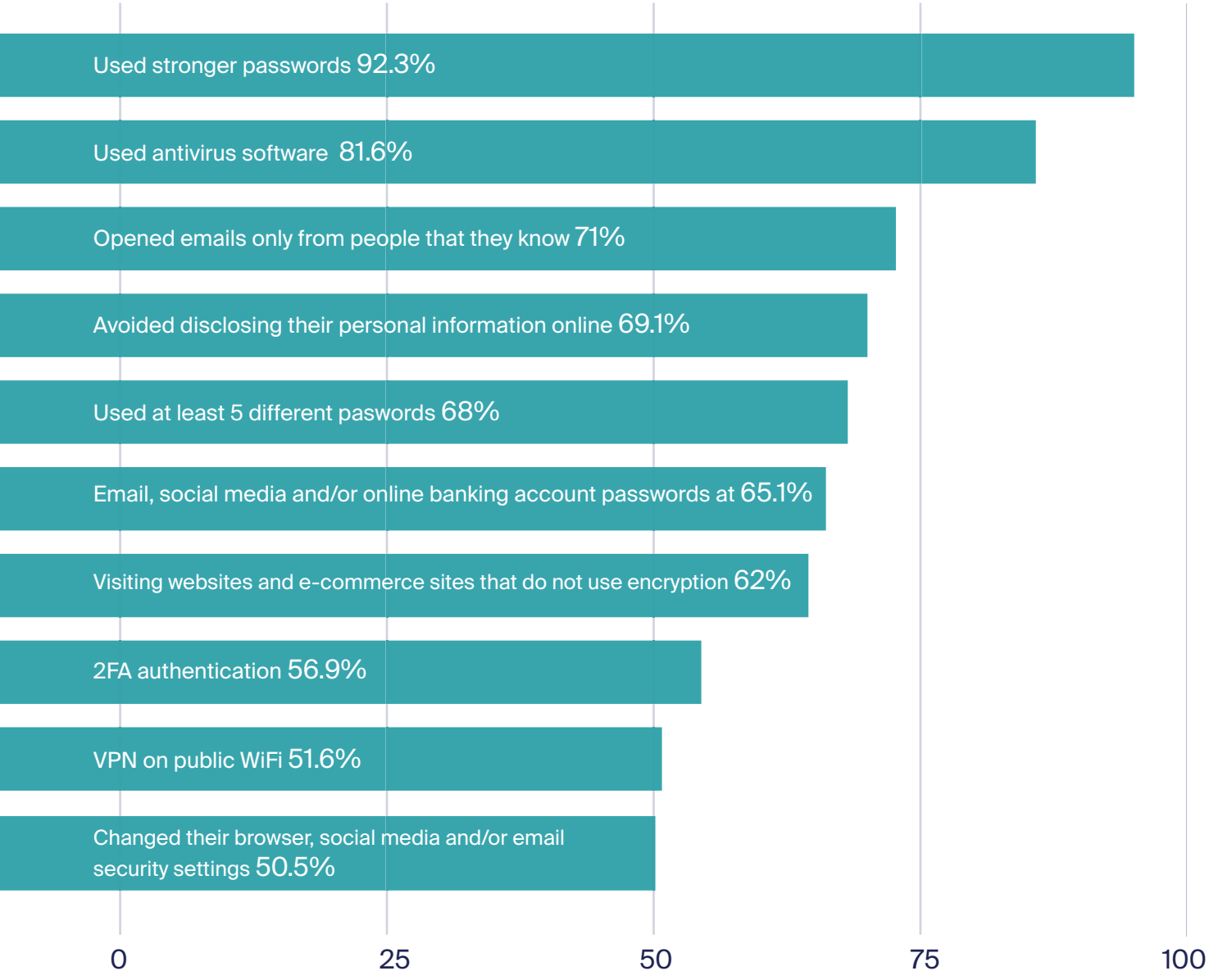
- NAS storage devices, DVRs, access point devices, wireless audio devices, servers are among the most attacked types of devices, but the users are not perceiving them as vulnerable
- Users perceive smart TVs, printers, thermostats, game consoles, doorbells as vulnerable
- Users do not put enough emphasis on mobile device security

Traditional Security Means

Most of the survey participants rely on traditional security means, such as strong passwords (92.3%), antivirus software (81.6%), or simply avoiding to disclose their personal information online (69.1%).

Surprisingly, only slightly more than half of participants (56.9%) have used 2FA authentication, while 51.6% have used VPN on public WiFi.

What have you done over the last 12 months to ensure protection from cyber threats?

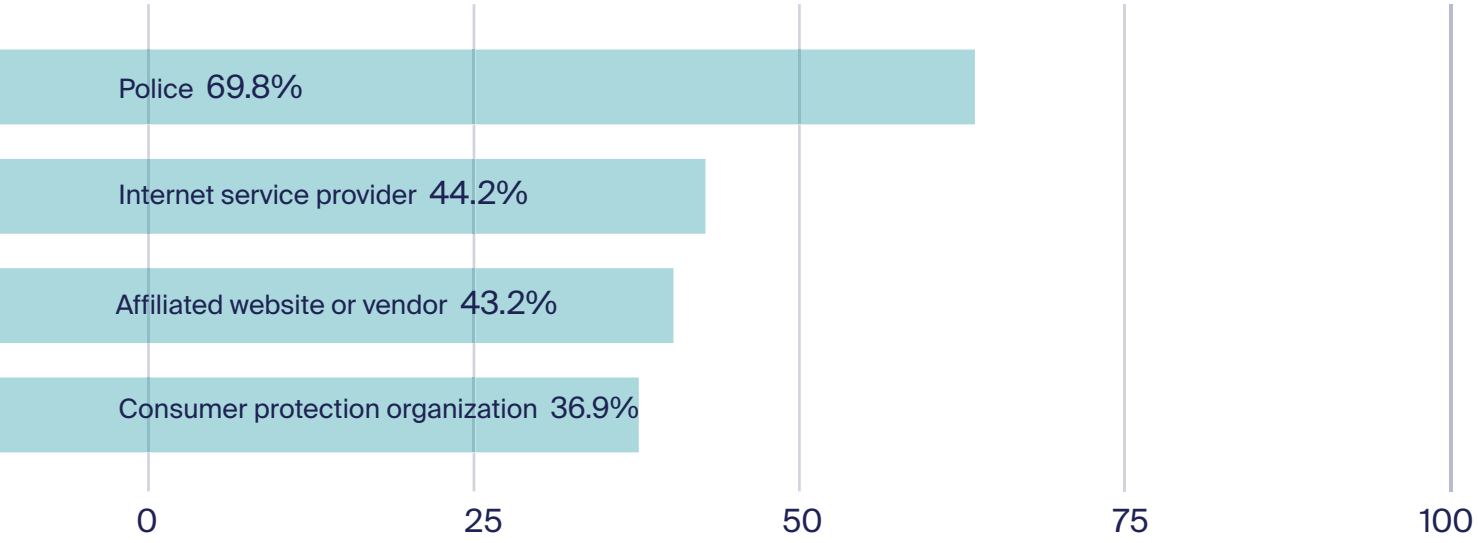


It's important to note that these methods do not address advanced types of cyber attacks that become more popular each year.

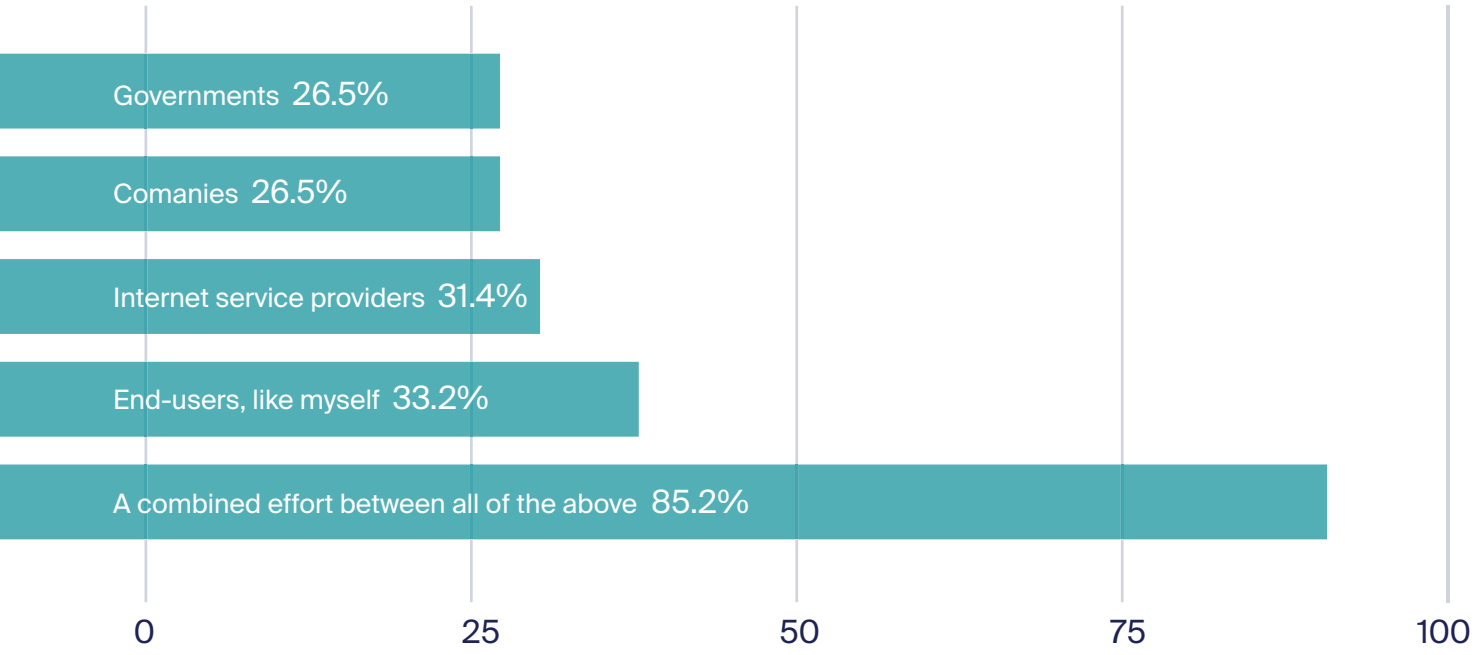
Responsibility for Protection

Who would you contact if you became a victim of cybercrime?

The end users are not entirely sure who should help them. If they became a victim of cyber-crime, 69.8% of respondents would contact police, 44.2% would reach out to their internet service provider, and 43.3% would get in touch with the affiliated website or vendor.



Who should be responsible for cybercrime prevention?

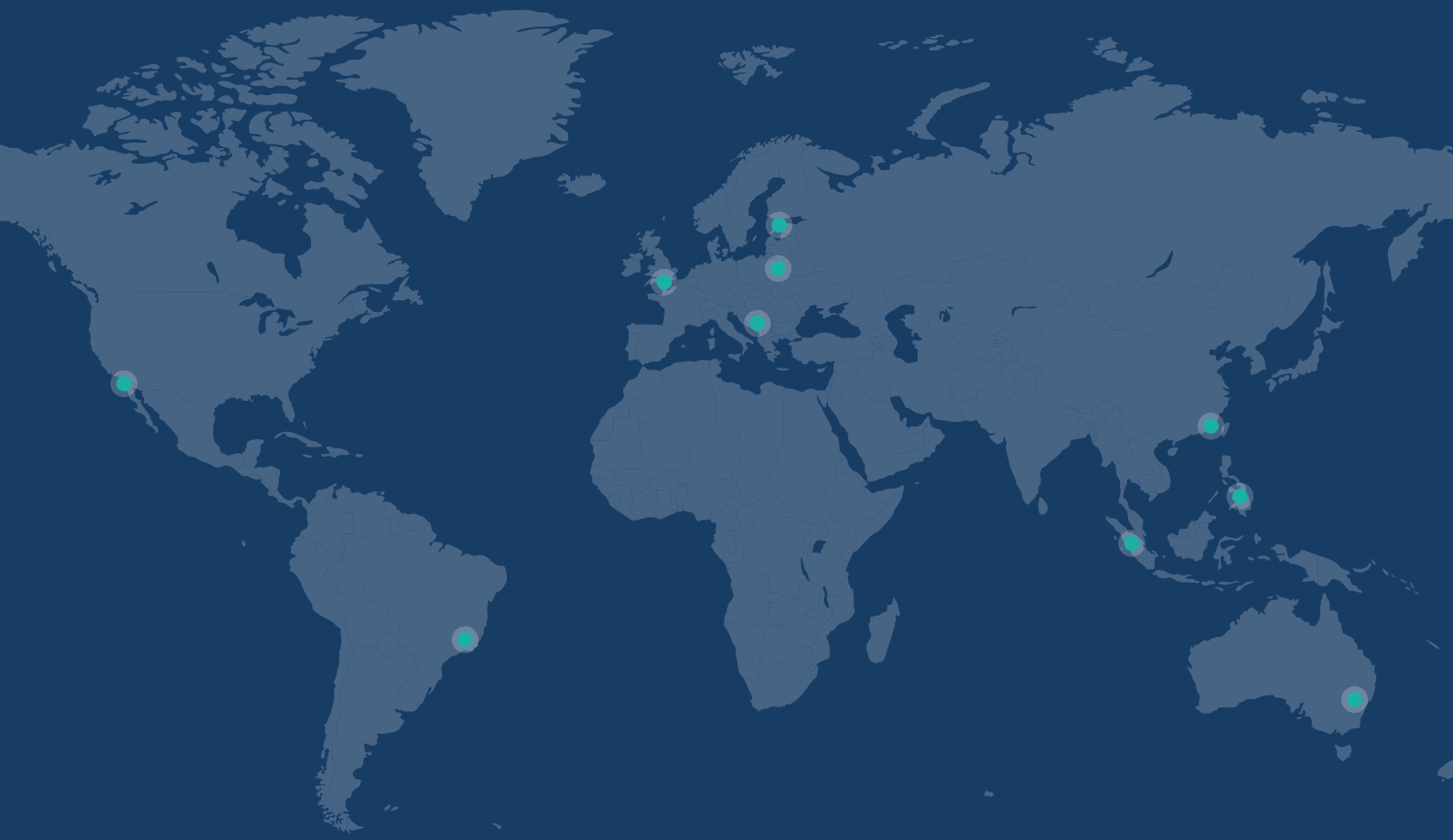


Around a third of survey participants think that either governments, companies, internet service providers, or end-users should be responsible for preventing cybercrime. But most (85.2%) of them agree that cybercrime prevention should be a combined effort between parties mentioned.

About CUJO AI

CUJO AI is the leading artificial intelligence company providing network operators AI-driven solutions, including AI security, advanced device identification, and content controls. CUJO AI Platform creates an intuitive end-user facing application for LAN and wireless (mobile and public WiFi), powered by machine learning and real-time data.

CUJO AI is recognized as a Technology Pioneer 2018 by the World Economic Forum. In 2018, it was listed as a “Vendor to Watch” and a “Cool Vendor in IoT security” by Gartner. The company has won the Security Solution of the Year award at the 2018 Glotel Awards.



Contacts

For media: pr@cujo.com
For sales: connect@cujo.com
cujo.com

CUJOAI