NORTON WI-FI RISK REPORT: U.S. Results

Research Objective

Norton by Symantec commissioned its second annual online survey, this year expanded to 15 global markets, in order to better understand consumers' public Wi-Fi perceptions and practices and to unveil consumer misconceptions and worries about the safety of these connections.
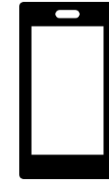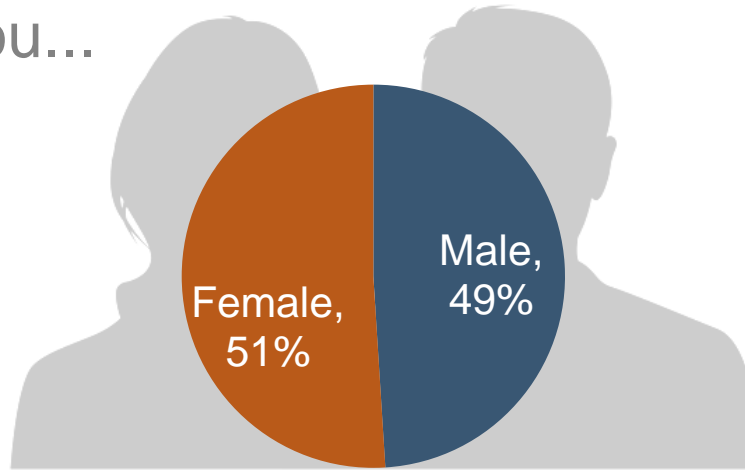
This survey explores consumers' knowledge about the safety of public Wi-Fi connections. While use of public Wi-Fi is nearly universal, most consumers are unaware of the dangers when connecting to public Wi-Fi and continue to put their personal information at risk. The survey's findings provide consumers with much needed context to make better decisions about protecting their personal information while using public Wi-Fi.

Methodology

- In May 2017, Norton by Symantec surveyed 15,532 mobile device users who had connected to Wi-Fi to discover their attitudes to and behaviors using public Wi-Fi.

- There were at least 1000 respondents from 15 global markets: Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Hong Kong, Mexico, Netherlands, New Zealand, United Arab Emirates, the United Kingdom and <u>USA</u>.
  - In the USA, there were 1002 respondents.

- The research was conducted by Norton by Symantec and Reputation Leaders through international online panel company Research Now. Data was collected from May 18th to June 5th, 2017.

- Quotas and subsequent weighting were applied to ensure that the respondent sample matched the most recent local census data for each market according to age, gender and region.

- The margin of error in total was 0.8% at a 95% confidence level, and 3.1% in each market

Demographics of the study (U.S.)

Are you...

Female, 51%
Male, 49%

1002 mobile Wi-Fi users in the USA

How old are you?

Age	Percent
18-24	13%
25-34	18%
35-44	18%
45-54	18%
55-64	19%
65 and over	14%

Which generation are you?

Generation	Percent
Traditionalists (72+)	4%
Boomer (53-71)	32%
Gen X (38-52)	24%
Millenial or Gen Y...	37%
Gen Z (18-20)	3%

4
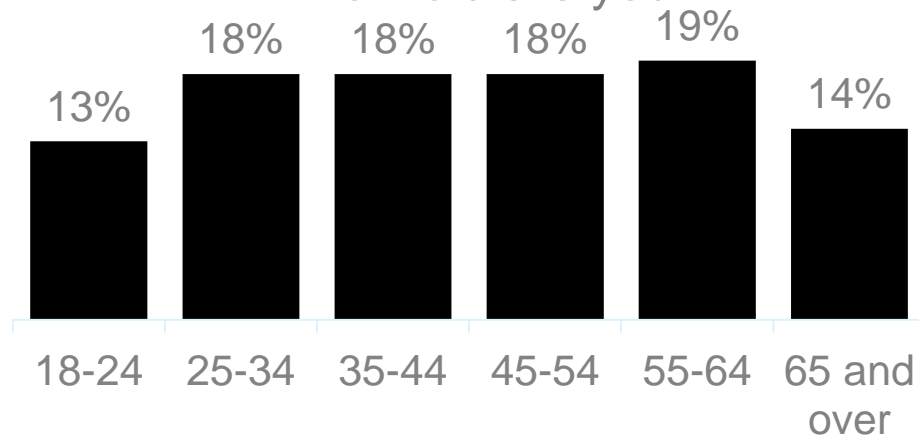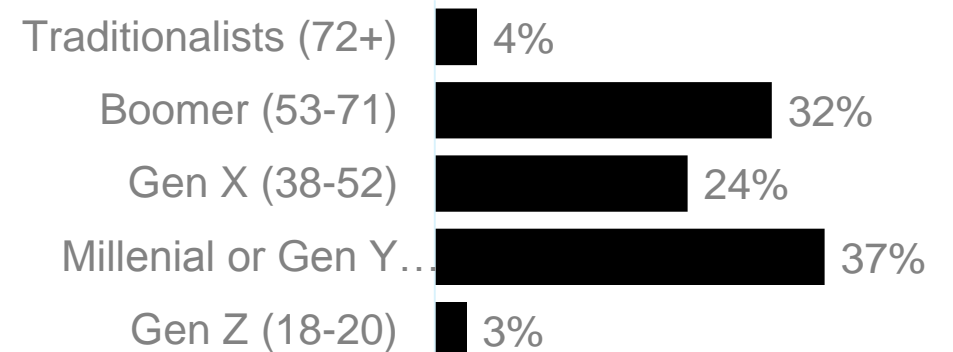
Key Findings: U.S.

- **Consumers are unable to resist a strong, free Wi-Fi network.**
  - Six in ten Americans (61 percent) wouldn't think twice about exchanging, sharing or even doing something to get access to a strong, free Wi-Fi network.
  - 35 percent have accessed a Wi-Fi network without the network owner's permission; 12 percent guessed or hacked the password.
  - 57 percent of Americans can't wait more than a few minutes before logging onto a Wi-Fi network or asking for the password after arriving at a friend's place, café, hotel or other location.

- **Even when travelling, access to public Wi-Fi is a must.**
  - Respondents say that access to a strong, free Wi-Fi network is a deciding factor when choosing the following:
    - A hotel/holiday/hostel rental (75 percent)
    - An airline (50 percent)
    - A place to eat or drink (café, bar, restaurant, etc.) (49 percent)
    - A transport hub for traveling and/or commuting (44 percent)
  - More than half (51 percent) of Americans say the most important reason for having access to a strong, free public Wi-Fi network is so they can use Maps, Google Maps or another GPS app to get around.

USA; Q12 Where did you use a public Wi-Fi network to view suggestive, semi-nude / nude photos, videos or other suggestive content?; base n = 219

Key Findings: U.S. (cont.)

- **Nevertheless, what some people choose to do over public Wi-Fi may surprise you.**

    – More than one in five Americans (22 percent) admit to having used public Wi-Fi to watch adult content.

    - Of those who admit to using public Wi-Fi to watch adult content, they've done so in the following locations:
        – Café/Restaurant (46 percent)
        – Work (45 percent)
        – Hotel/Airbnb (39 percent)
        – Airport (37 percent)
        – Public restroom (23 percent)
        – On the street (20 percent)
        – Train/bus station (19 percent)

Key Findings: U.S. (cont.)

- **Consumers' dependency on public Wi-Fi is putting their personal information at risk. What someone thinks is private on his or her personal device could easily be accessed by cybercriminals through an app with potential privacy vulnerabilities or an unsecure Wi-Fi network.**
  - Nearly 70 percent feel their personal information is safe when using public Wi-Fi, yet 41 percent can't tell the difference between a secure or unsecure public W-Fi network.
  - 73 percent of Americans don't use a Virtual Private Network (VPN) to secure their Wi-Fi connections, even though it's considered one of the best ways to protect your personal information.
  - 92 percent of Americans have potentially put their information at risk while using public Wi-Fi.

- **When consumers think about a hacker or malicious person stealing their personal information and posting it online, emotions run high.**
  - 40 percent would feel horrified if the details of their bank accounts and financial information were posted online; 45 percent would feel worried.
  - 40 percent would feel angry if their photo library, including intimate, personal and family photos were posted online.
  - 33 percent would be worried if their children's schedule, location or academic details were posted online.
  - 19 percent would be embarrassed if the details of their private chats/texts conversation were posted online.

Key Findings: U.S. (cont.)

- **Though their actions may say otherwise, consumers are not invincible on public Wi-Fi. But there are ways to better ensure your personal information doesn't get into the wrong hands.**

  - Take Protective Measures: One of the best ways to protect your information online is to use a Virtual Private Network (VPN) from a trusted vendor. VPNs provide a "secure tunnel" that encrypts data being sent and received between your device and the internet.

  - Do HTTPS: Many companies use secure websites — HTTPS (Hypertext Transfer Protocol Secure) — to provide online security. You can tell if a website is secure if it has "https" in its URL and has a small lock symbol next to it. However, even though the website itself might be safe, your personal information could still be vulnerable if your network connection isn't secure.

  - Sharing Less Is Best: Think twice before entering any type of personal information – from passwords, to financial details and photos – over public networks. Even if you're not actively sharing the information, your device may be doing so for you. Many devices are programmed to automatically seek connections to other devices on the same network, which could cause your files to be vulnerable. Be sure to disable sharing on your devices to ensure what's yours stays yours.
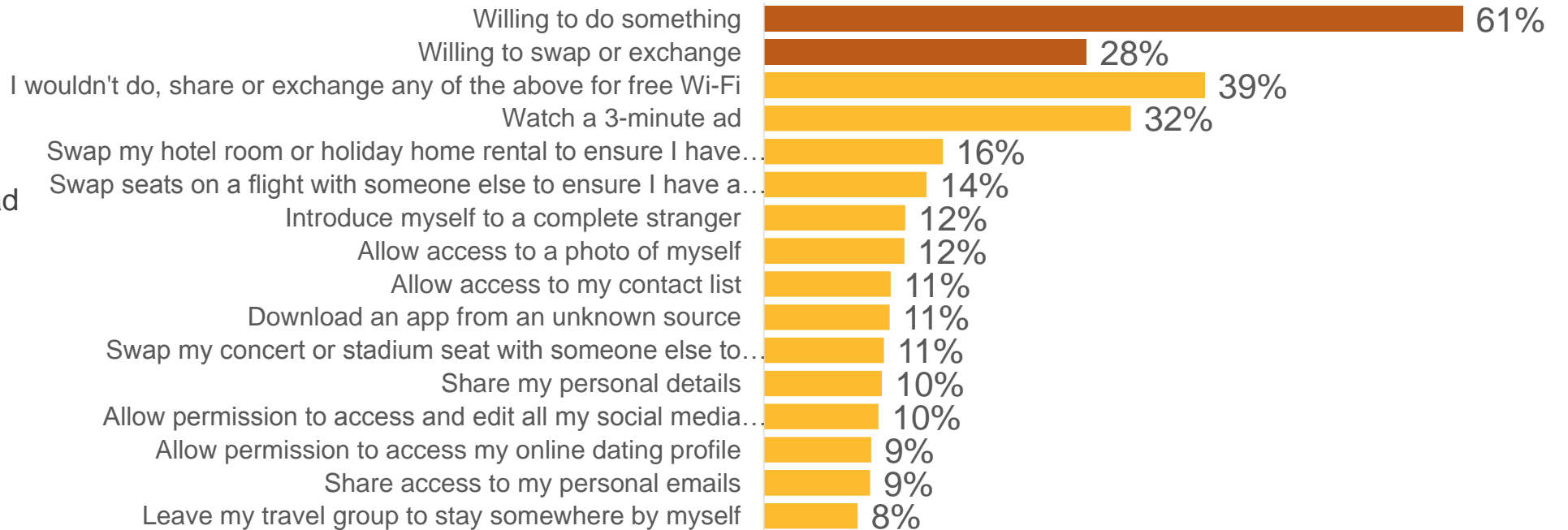
Detailed Findings

Americans love free Wi-Fi – 61% wouldn't think twice about exchanging, sharing or even doing something to get a strong, free signal

What would you be willing to exchange and/or do to secure a free Wi-Fi connection with a strong signal when travelling, on holiday or at a concert or stadium event?

Nearly 1 in 3
would be willing to watch a 3-minute ad

1 in 10
would be willing to share personal details

Willing to do something	61%
Willing to swap or exchange	28%
I wouldn't do, share or exchange any of the above for free Wi-Fi	39%
Watch a 3-minute ad	32%
Swap my hotel room or holiday home rental to ensure I have…	16%
Swap seats on a flight with someone else to ensure I have a…	14%
Introduce myself to a complete stranger	12%
Allow access to a photo of myself	12%
Allow access to my contact list	11%
Download an app from an unknown source	11%
Swap my concert or stadium seat with someone else to…	11%
Share my personal details	10%
Allow permission to access and edit all my social media…	10%
Allow permission to access my online dating profile	9%
Share access to my personal emails	9%
Leave my travel group to stay somewhere by myself	8%

USA; Q6 What would you be willing to exchange and/or do to secure a free Wi-Fi connection with a strong signal when travelling, on holiday or at a concert or stadium event?
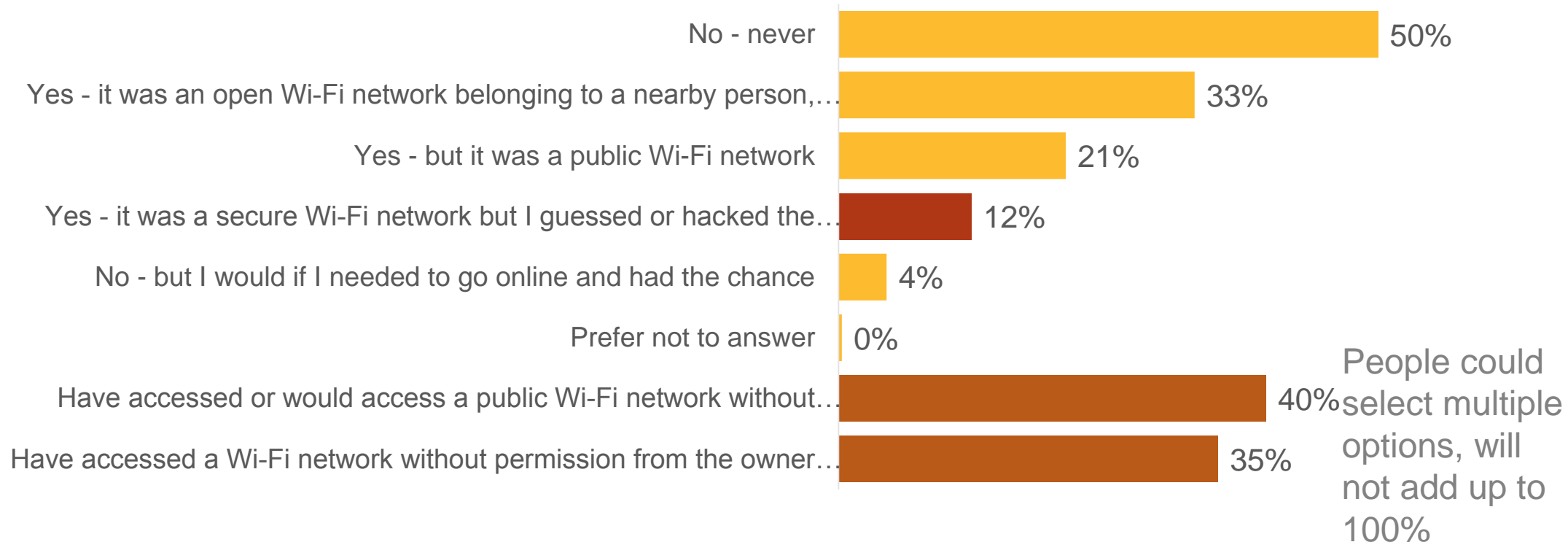
Sometimes they don't ask – 35% have accessed a Wi-Fi network without the owner's permission, and 12% guessed or hacked the password

Have you ever accessed someone else's Wi-Fi network from your device without their permission?

No - never	50%
Yes - it was an open Wi-Fi network belonging to a nearby person,…	33%
Yes - but it was a public Wi-Fi network	21%
Yes - it was a secure Wi-Fi network but I guessed or hacked the…	12%
No - but I would if I needed to go online and had the chance	4%
Prefer not to answer	0%
Have accessed or would access a public Wi-Fi network without…	40%
Have accessed a Wi-Fi network without permission from the owner…	35%

People could select multiple options, will not add up to 100%

USA; Q5 Have you ever accessed someone else's Wi-Fi network from your device without their permission?

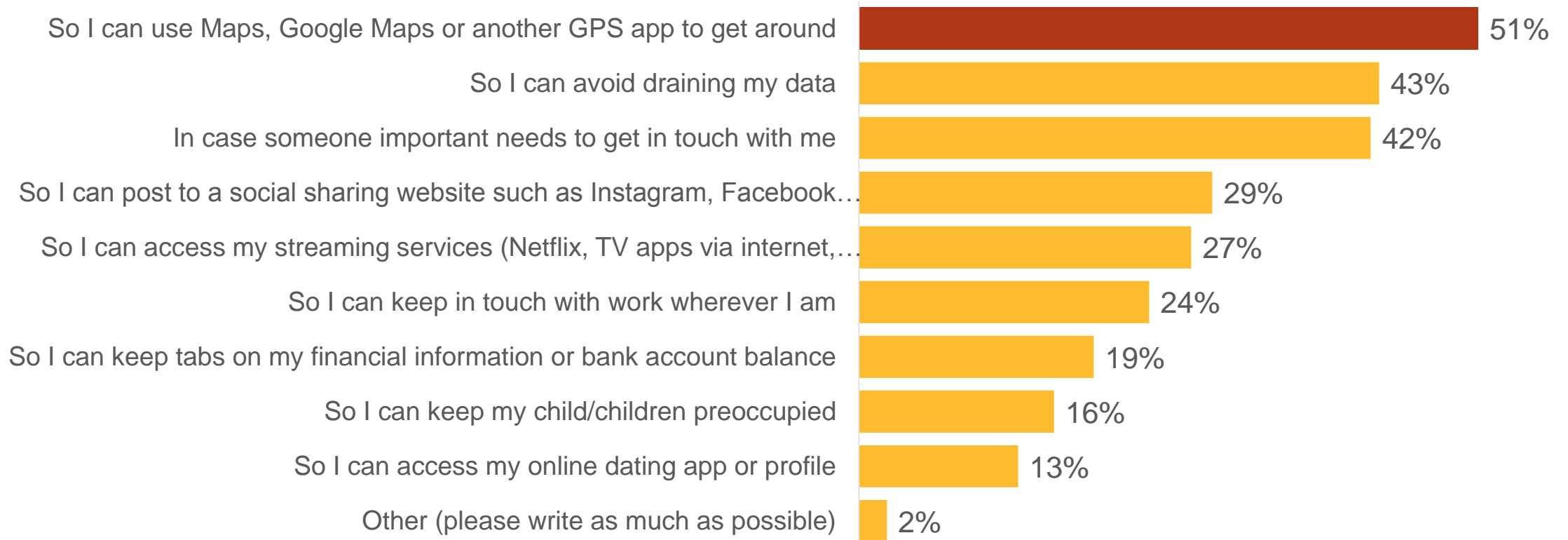# Even when travelling, access to public Wi-Fi is a must for Americans

Is access to a strong Wi-Fi signal a deciding factor for you when choosing the following services:

| Service	Percentage
A hotel/hostel/holiday rental	75%
An airline	50%
A place to eat or drink (café, bar, restaurant, etc.)	49%
A transport hub for traveling and/or commuting	44%
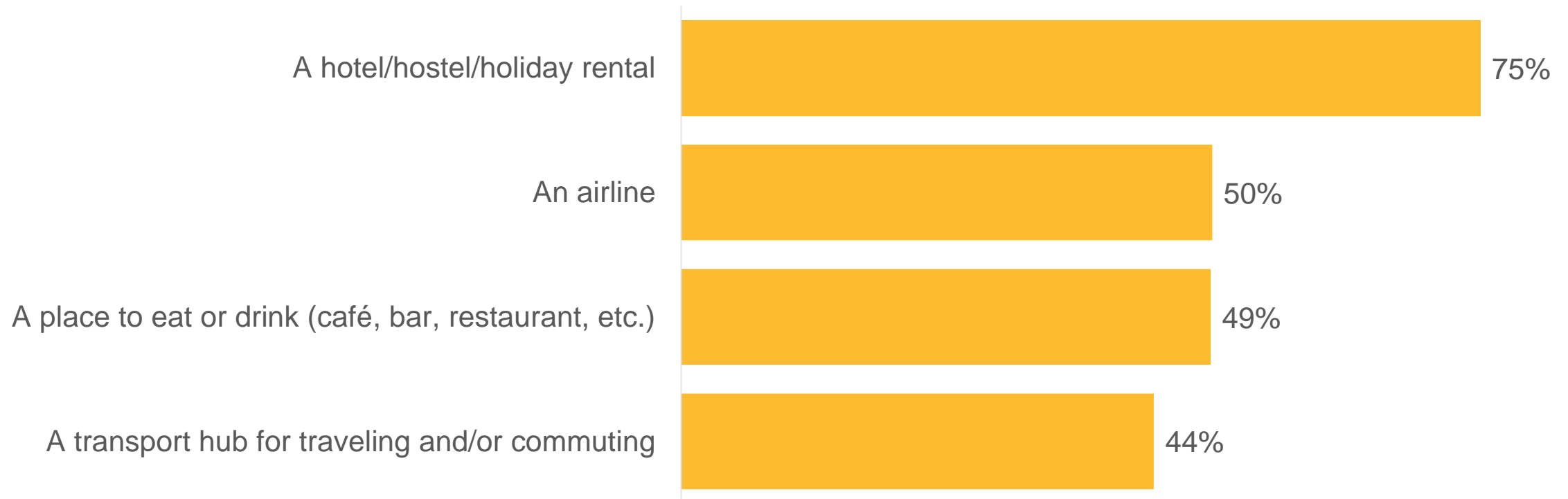
Over half of Americans say strong public Wi-Fi for Maps or GPS is most important

In these situations, what do you consider the most important reason for having access to a strong, public Wi-Fi connection?

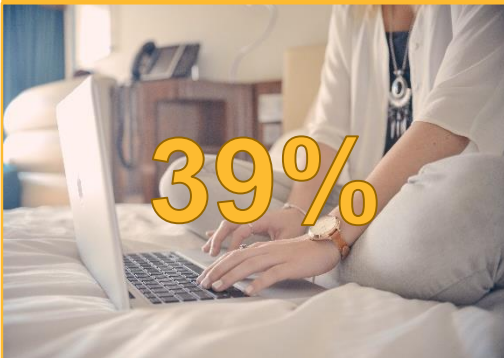| Reason	Percentage
So I can use Maps, Google Maps or another GPS app to get around	51%
So I can avoid draining my data	43%
In case someone important needs to get in touch with me	42%
So I can post to a social sharing website such as Instagram, Facebook…	29%
So I can access my streaming services (Netflix, TV apps via internet,…	27%
So I can keep in touch with work wherever I am	24%
So I can keep tabs on my financial information or bank account balance	19%
So I can keep my child/children preoccupied	16%
So I can access my online dating app or profile	13%
Other (please write as much as possible)	2%

Generations place differing values on Wi-Fi – 63% of Gen Z say the most important reason for public Wi-Fi is to post on social media

In these situations, what do you consider the most important reason for having access to a strong, public Wi-Fi connection by which generation are you?

Chart data:
- Total: 29%
- Gen Z (18-20): 63%
- Millenial or Gen Y (21-37): 36%
- Gen X (38-52): 29%
- Boomer (53-71): 17%
- Traditionalists (72+): 9%

■ So I can post to a social sharing website such as Instagram, Facebook or Snapchat

USA; Q7 In these situations, what do you consider the most important reason for having access to a strong, public Wi-Fi connection?
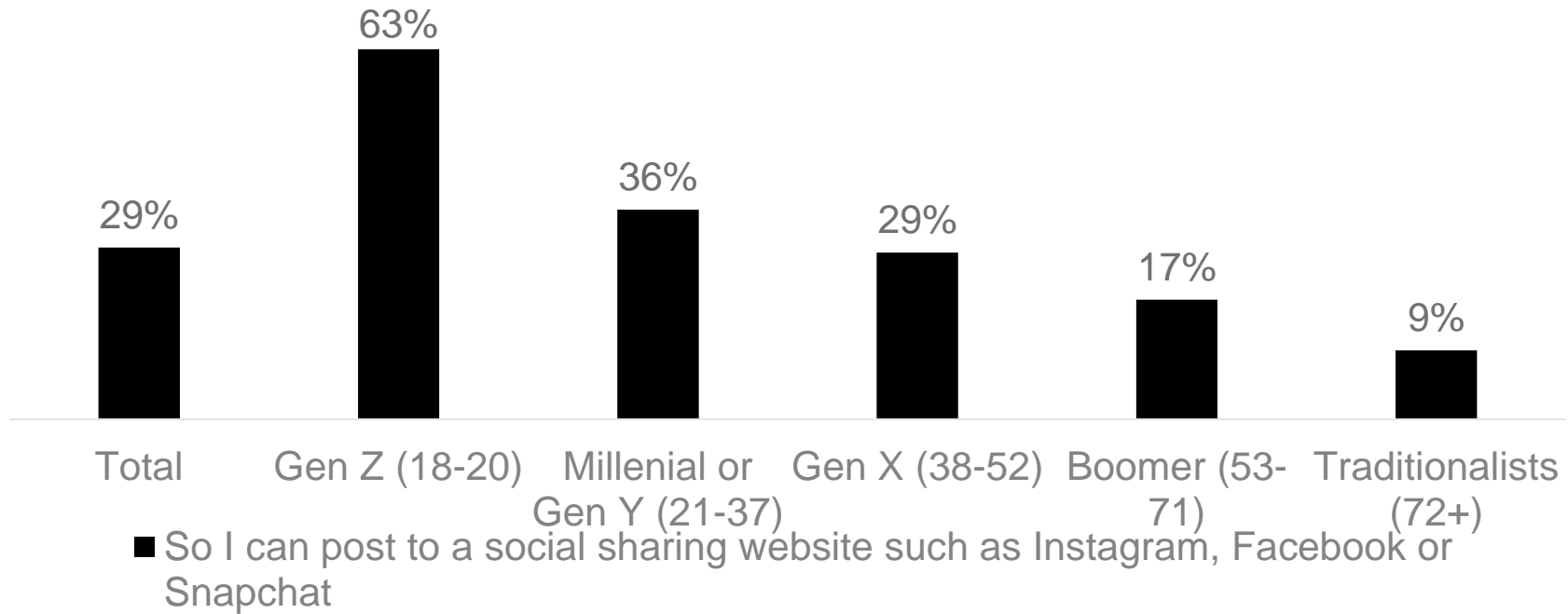
Nevertheless, what people do on public Wi-Fi may surprise you

More than one in five Americans admit to using public Wi-Fi to watch adult content. They've done so in the following locations:

| 39%	38%	46%	45%	37%
Hotel/Airbnb	At a friend's	Café/Restaurant	Work	Airport
20%	19%	29%	23%	21%
On the street	Train/bus station	Library	Public toilets	School

However, Americans have a false sense of security – 69% feel their personal information is safe when using public Wi-Fi

More than one in four (28 percent) feel their personal information is <u>very safe</u> when using public Wi-Fi connections.
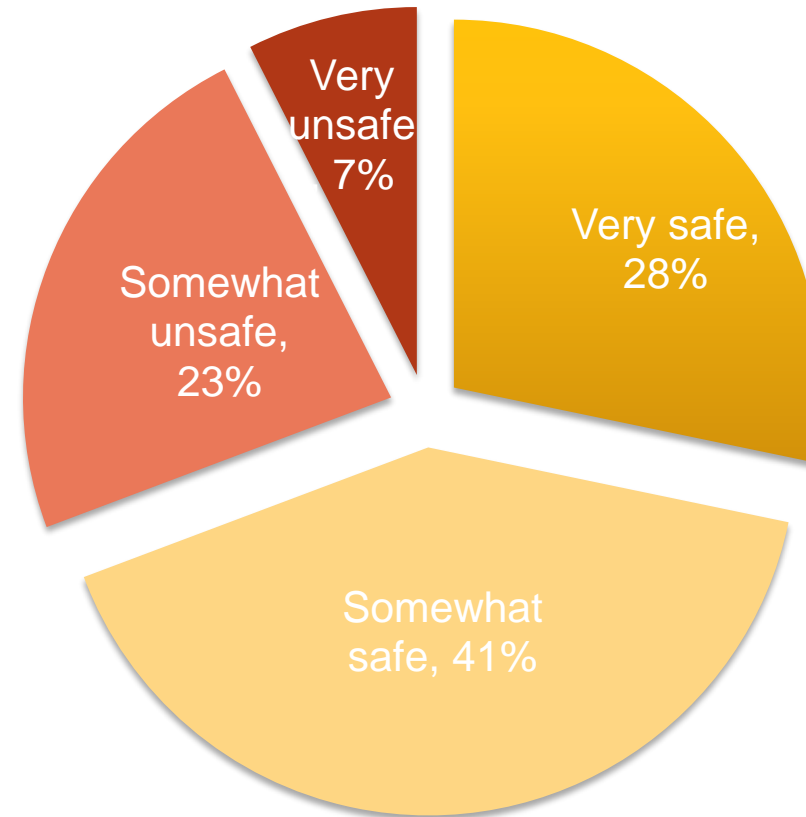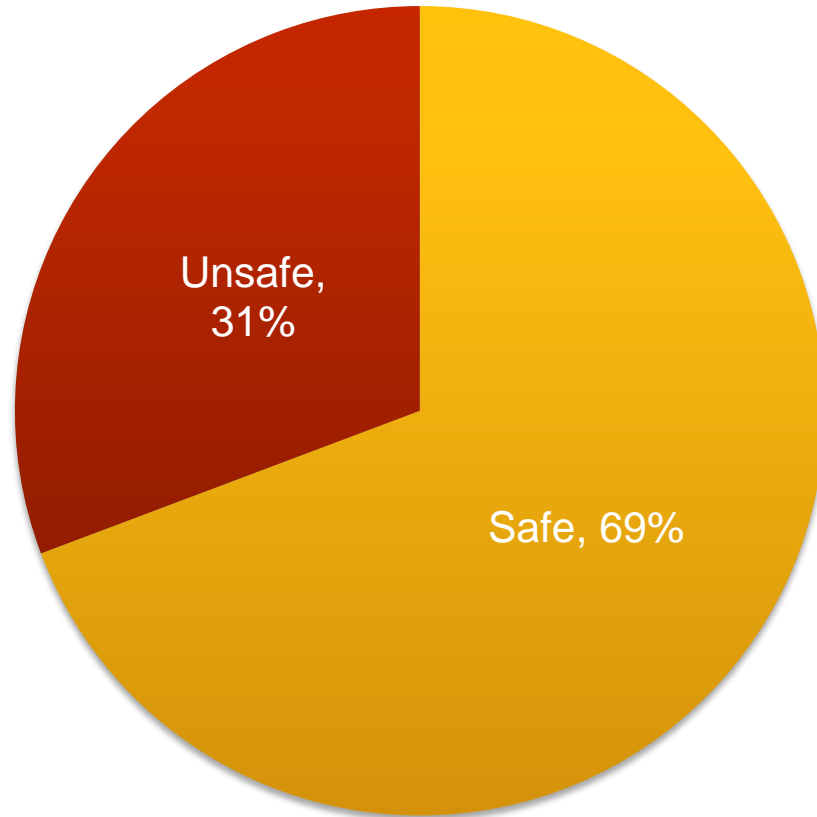
73% of Americans don't use a Virtual Private Network (VPN) to secure their Wi-Fi connections

While nearly **three quarters** of Americans are familiar with VPNs, only **one third** of those people choose to use a VPN to protect their personal information.

Do you use a VPN every time you use Wi-Fi?

Yes, 27%

No, 49%

I never heard of VPN before today, 24%
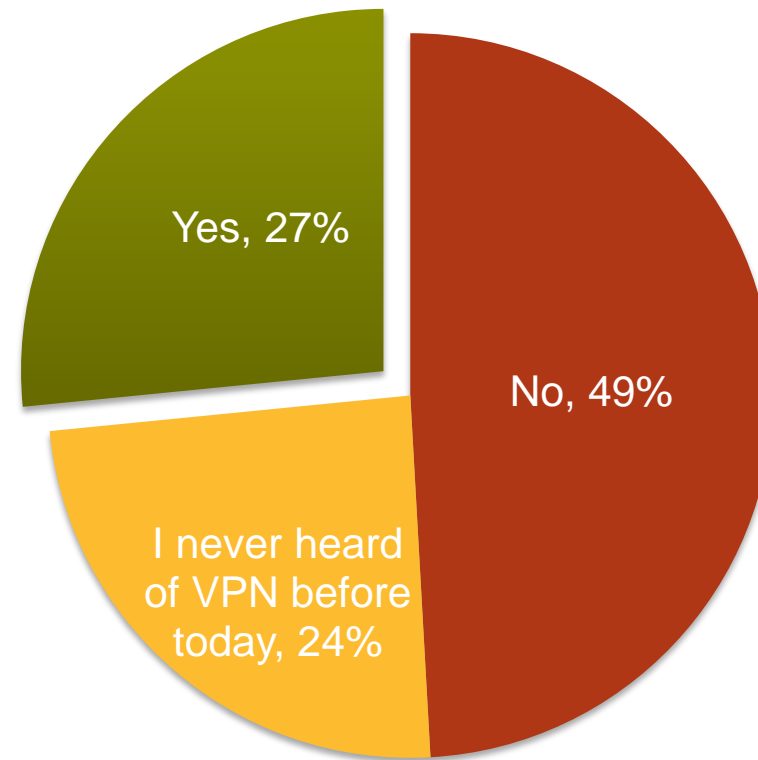
92% of Americans admit to taking security risks on public Wi-Fi, such as accessing personal email, bank accounts or financial information

Have acted in some way	92%
Logged into my personal email account	62%
Logged into my social media account(s)	56%
Shared photos or videos	48%
Checked my bank account or accessed financial information	32%
Logged into my work email account	29%
Sent a work document (e.g., planning document, financials)	24%
Shared travel plans or location information	23%
Provided my credit card details (e.g., when online shopping)	22%
Logged onto other accounts using a password	22%
Entered personally identifiable information (e.g., social security number, birthday,…	19%
Managed my connected home device (e.g., thermostat, home entry, baby monitor,…	13%
None of the above	8%

92% Have taken risks on public Wi-Fi

USA; Q4 Which of the following have you done on your mobile phone, tablet or laptop while connected to a public Wi-Fi network?

How would you feel ?

if a hacker or malicious person stole personal information
from your mobile phone, tablet, or laptop and posted it publicly online?

Horrified	Angry	Worried	Embarrassed	Neither worried nor horrified
Details of your bank accounts and financial information	Your photo library incl. intimate, personal and family photos	Your children's schedule, location or academic details	Details of private chat/text conversations	News sites you visit or political preferences
40%	40%	33%	19%	35%