SOPHOS
Cybersecurity evolved.

The State of Consumer Home Cybersecurity 2021

A Sophos Whitepaper. July 2021

The overwhelming majority of Americans are concerned about their online security – and cyber threats like malware and identity theft, in particular. In the last year, changes brought on by the pandemic further escalated concerns for many.

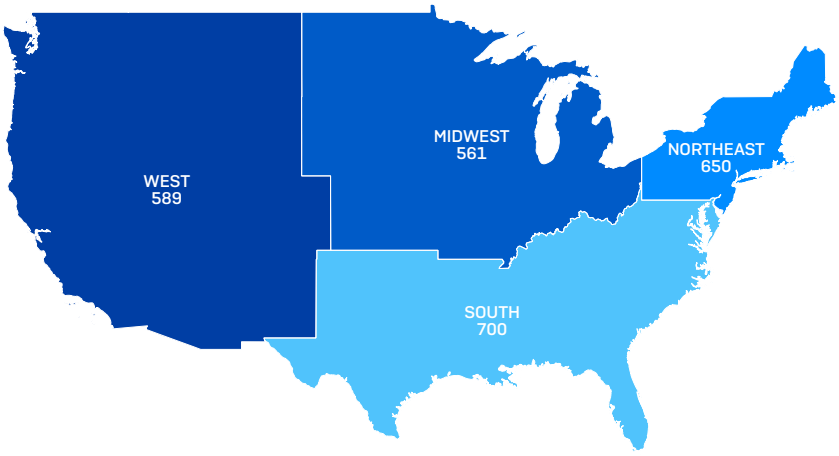
To understand the realities of consumer home cybersecurity, Sophos commissioned an independent survey of 2,500 consumers across the nation. The findings provide new insight into consumer security preparedness (or lack thereof), revealing that many consumers are woefully uninformed about threats – like ransomware; the likelihood and risk of these threats within their homes; and how to protect themselves and their families against them.

Interestingly, the findings reveal a false sense of security among many consumers. Perceived levels of security knowledge are inaccurately high with a significant number of consumers thinking they know more about security than they actually do.

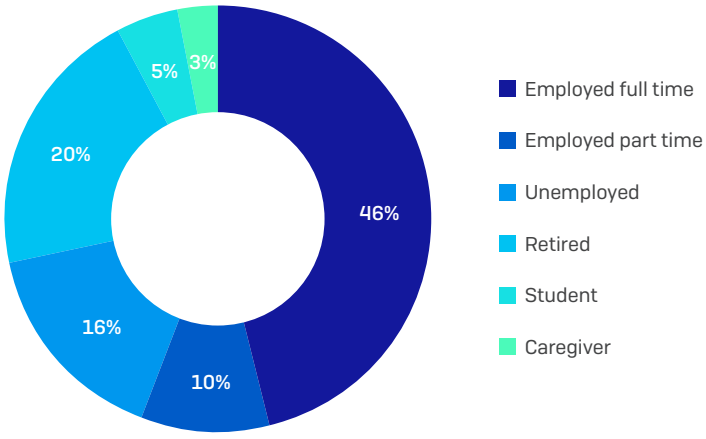
About the Survey

Sophos commissioned research specialist Vanson Bourne to survey 2,500 consumers across all regions of the U.S. on their firsthand experiences with threats, security concerns, and the steps they're taking to manage household devices and secure individuals within their homes. Sophos had no role in the selection of respondents, and all responses were provided anonymously. The survey was conducted in February 2021.

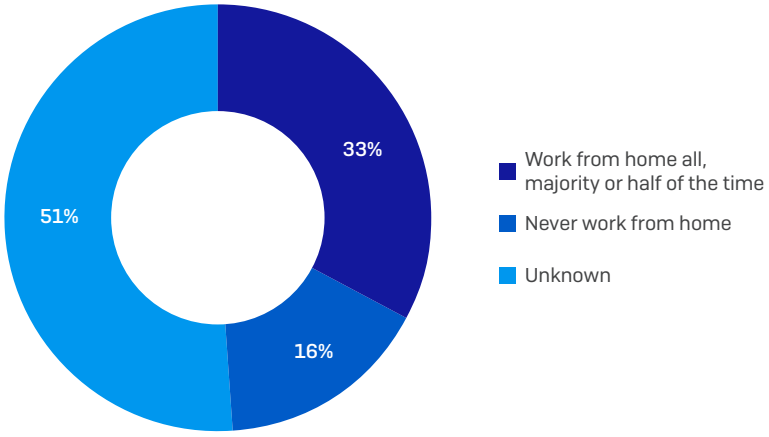
Respondents were all based in the United States, spread out across four defined regions.



Respondents were equally split by age and gender. Respondents also came from a range of employment types.

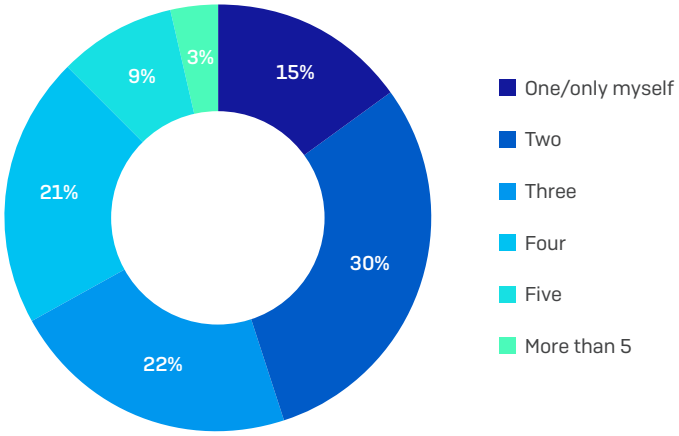


Of those who were employed (full and part time), the majority work from home at least half of the time.

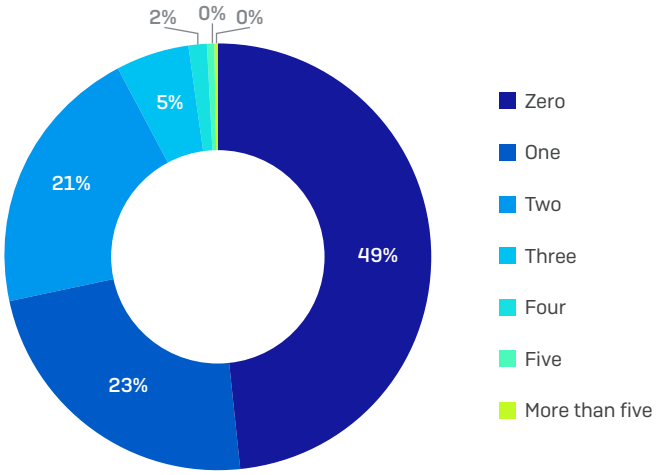


Respondents varied based on the number of people – including children under 18 years old – in their household.

Number of people in household

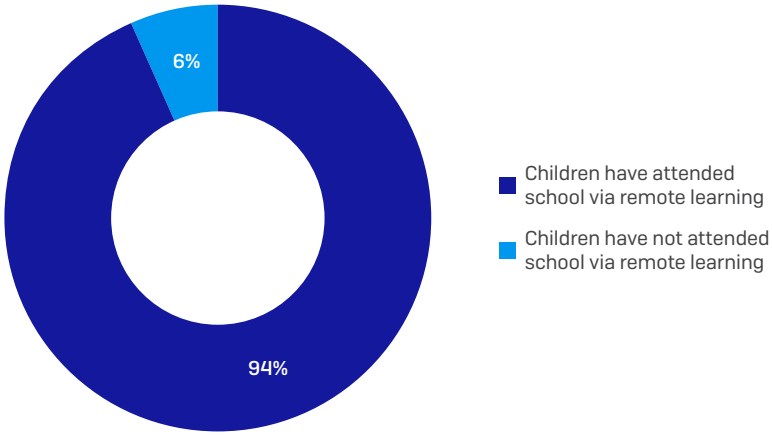


Number of children (<18 years old) in household:



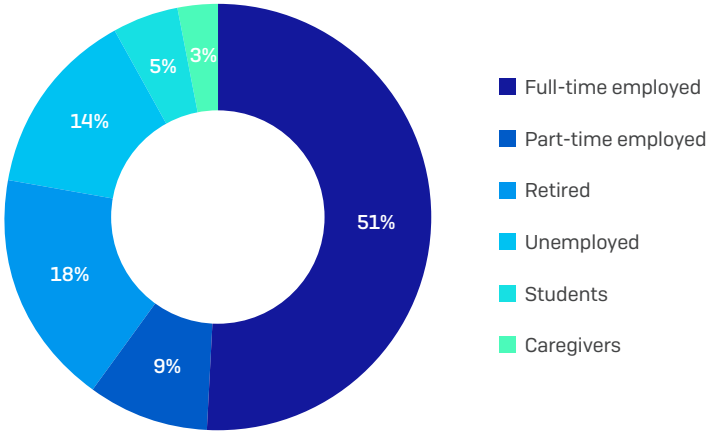
Only asked to respondents who have other people living in their household.

Of those with children in their household, nearly all have had children attend school via remote learning in some capacity since the start of the COVID-19 pandemic.

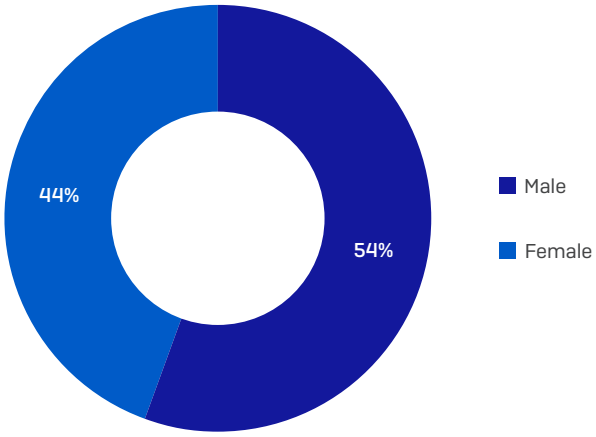


Most respondents have a designated "IT boss" for their household – the "IT boss" being an individual tasked with managing IT devices within and outside of his/her household. The employment, gender and age breakdowns of IT bosses are as follows:

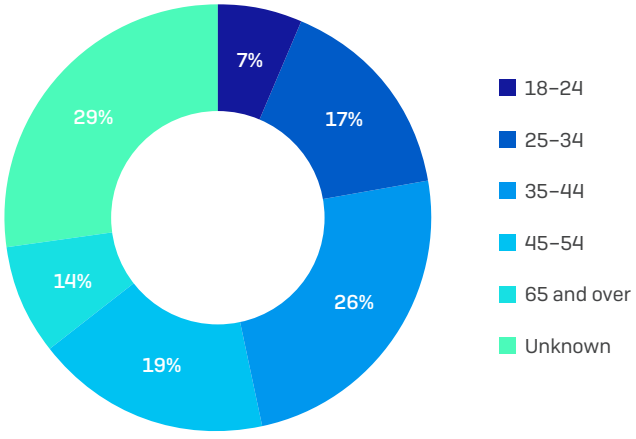
Employment status of IT bosses



IT bosses are...



Age ranges of IT bosses



Key Findings

Survey findings provide new insight into consumer experiences with threats; online security concerns, which have grown throughout the pandemic; and security practices that are falling short.

Consumers are increasingly concerned about their online security and imminent attacks

- 91% of consumers are worried about online security threats affecting their household
  - Consumers are most worried about viruses and malware (60%), identity theft (55%), financial fraud (48%), and ransomware (45%)
  - Government monitoring is at the bottom of the list (26%)
  - Among just parents (defined as respondents with children in their household), the number one concern is inappropriate content (39%)
- 61% believe that either they or someone else in their household could be the target of an online attack in the next 12 months
- 45% believe they're more at risk of being hit by an attack now than 12 months ago
- 69% believe that working from home introduces new security risks as computing devices on the same home Wi-Fi network may enable unauthorized access to data on connected devices
- When it comes to ransomware specifically, 18% of respondents report that someone in their household has personally suffered from a ransomware attack, nearly half of which occurred in the last year
  - Among those who reported ransomware attacks and were able to correctly identify what ransomware is:
    - The majority (62%) did not pay the ransom; only 29% paid the ransom
    - The most significant impacts of ransomware attacks included needing to upgrade security solutions (35%), the inability to use devices for personal use (28%), temporary data loss (30%), and financial loss (24%)

Security practices are falling short for many consumers – especially when it comes to securing devices used by children

- 18% don't spend any time managing household devices
- 20% never backup data to the cloud
- 24% don't have or use a password manager
- 36% don't update or patch their operating system and applications when prompted, or check to do so at least weekly
- 46% don't regularly run antivirus and malware scans
- Just 35% of parents have set up separate user accounts on devices that their children use, and only 44% have user passwords set up at all on these devices
- Only half (50%) of parents have added parental controls on devices that their children use, and only 42% have set up safe browsing or a web content filter

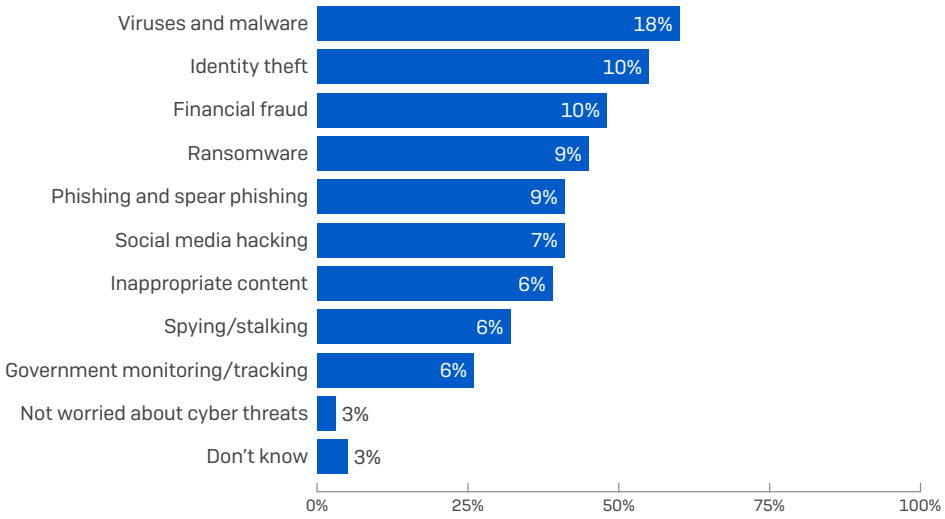
Consumer security knowledge varies – for many, self-perceived levels of knowledge are inaccurately high

- Nearly a quarter of respondents (24%) falsely believe that Apple macOS is not affected by cyberattacks
- Awareness of what ransomware actually is varies – and only 49% could correctly identify it, indicating that a lack of cybersecurity knowledge leads many to falsely interpret their experience as a true ransomware attack
- Cybersecurity knowledge varies by U.S. region
  - Respondents in the Northeast report having the best knowledge (50% say they know a lot about cybersecurity)
    - However, more than half of these respondents (53%) were unable to correctly identify ransomware from other online threats
  - Respondents in the South admit to having the worst cybersecurity knowledge (19% say they know little to nothing about cybersecurity)
  - Among those in the West and Midwest, 41% and 40% respectively say their cybersecurity knowledge is good; 17% in both regions say their knowledge is poor
- Most households (83%) have at least one person designated as the "IT boss" to manage security on all devices in the household
  - More than half of households have one single IT boss
  - 22% of households have IT boss responsibilities shared between two people
  - Only 10% of households say they have no IT boss overseeing their devices

Part 1: Consumers are increasingly worried about their online security and imminent attacks

More than 9 in 10 worry about online security threats at home

An overwhelming 91% of consumers said they are worried about online security threats affecting their household. The specific threats they are most concerned about include:

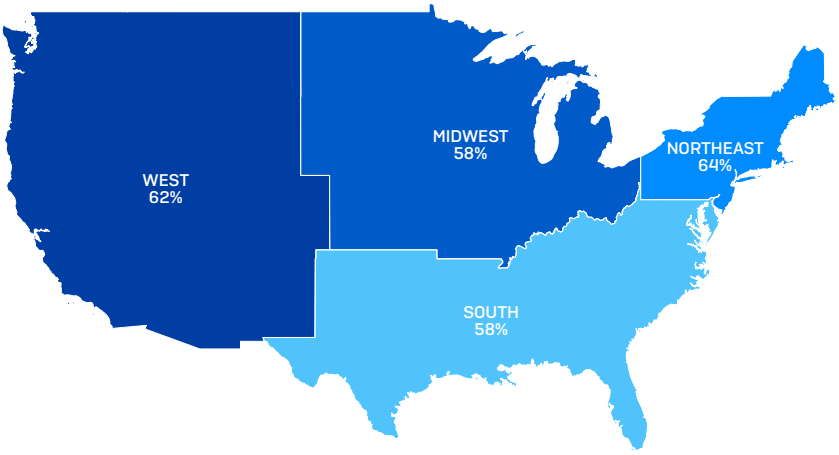


For parents, the number one concern is inappropriate content.

The majority of consumers believe they're likely to be the target of online attacks

Most people (61%) believe they or someone else in their household could be the target of an online attack in the next 12 months.

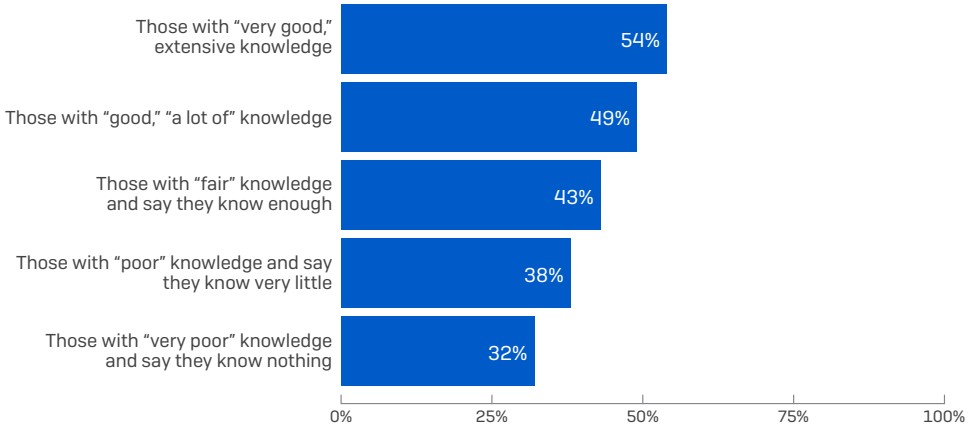
These fears vary based on geography and online security knowledge. More than six in 10 people living in the Northeast and West believe they could be the target of an online attack; less than six in 10 in the Midwest and South felt the same.



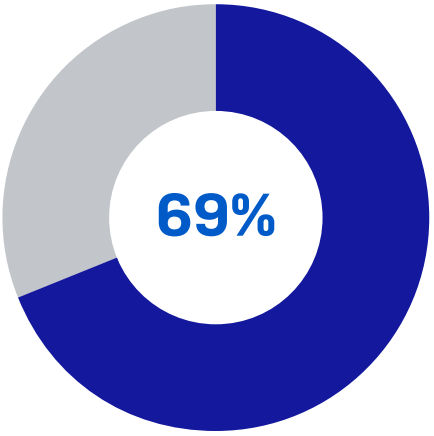
Online risk level: Now vs. 12 months ago

While a majority of respondents believe they are now at greater risk of an online attack than 12 months ago, this varies based on security knowledge levels. The greater a respondent's perceived level of cybersecurity knowledge, the more they believe their risk had grown in the past 12 months; the lower a respondent's cybersecurity knowledge, the less likely they were to believe they were at greater risk now.

As a result, there is a 22-point difference between consumers with "very good" and "very poor" levels of cybersecurity knowledge in believing their cyber risk levels have grown in the last 12 months.



This risk perception may be heightened by a year of working from home. Nearly seven in 10 consumers believe that working from home introduces new security risks, as computing devices on the same home Wi-Fi network may enable unauthorized access to data on connected devices.



believe working from home increases security risks

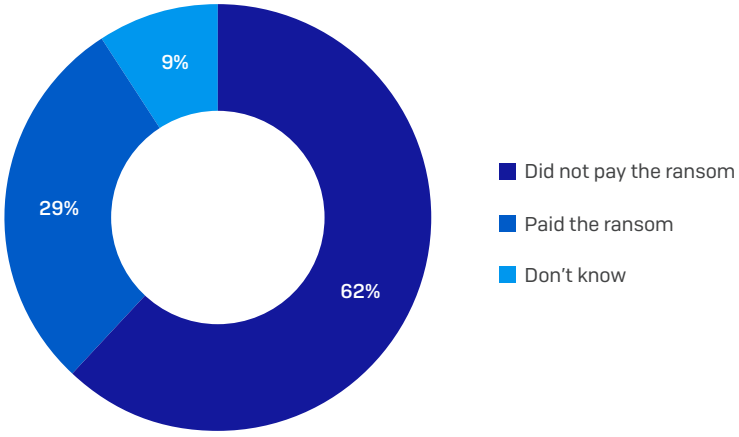
Nearly 1 in 5 consumers have firsthand experience with ransomware

One online security threat on the minds of many consumers is ransomware. Eighteen percent of respondents said that someone in their household has personally suffered from a ransomware attack. Nearly half of those attacks occurred in the last year.

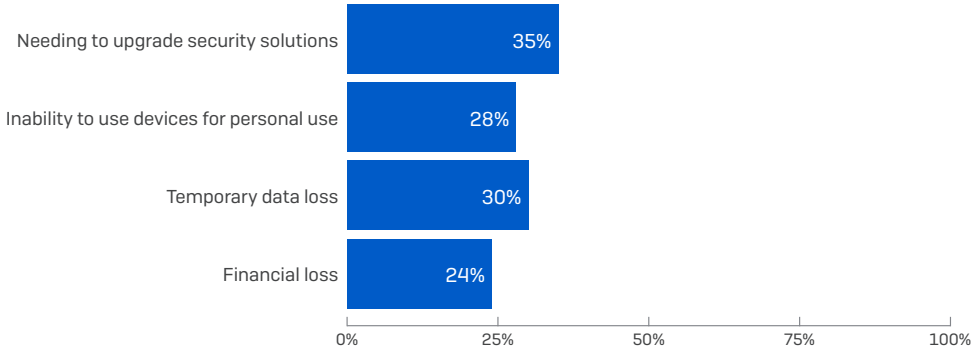
Incidence of ransomware attacks varies by geography. The number of consumers who were the victim of ransomware were more likely to be in the Northeast (22%) – this is despite the fact that the Northeast also boasts the highest level of perceived online security knowledge.

By contrast, consumers in the West, Midwest, or South reported a lower rate of suffering from a ransomware attack – 18%, 17%, and 15%, respectively.

Of the 18% of respondents who reported experiencing a ransomware attack on their household and were also able to correctly identify ransomware, there was a nearly two-to-one split between those who did not pay the ransom and those who did.



The most significant impacts of ransomware attacks included:

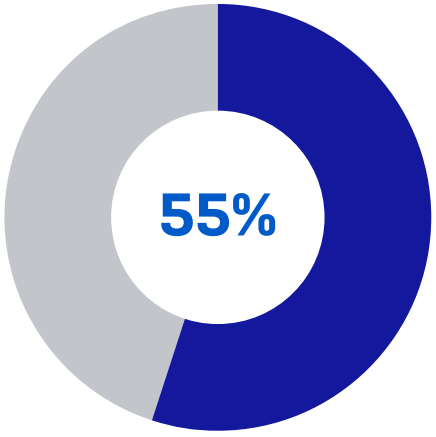


Part 2: Security practices are falling short for many consumers – especially when it comes to securing devices used by children

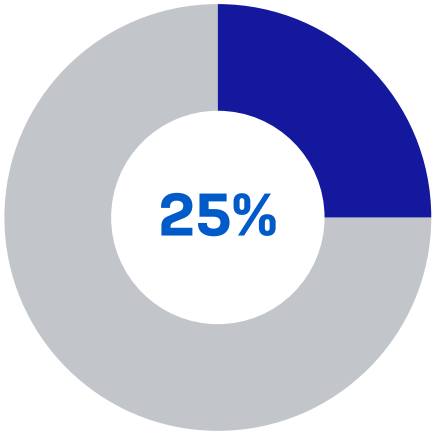
The average U.S. household carries many devices – more personal than company-owned or school-issued

Households surveyed own an average of four personal devices. The number of company-owned or school-issued devices per household was far lower – just one in each category.

4 personal devices (on average) per household



of respondents who are employed or have another person in their household have **0** company-owned devices; **23%** have **1**

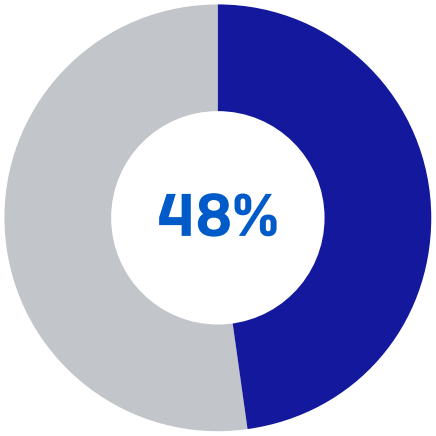


of respondents who have children under 18 years old in their households have **0** school-issued devices; **36%** have **1**; **24%** have **2**

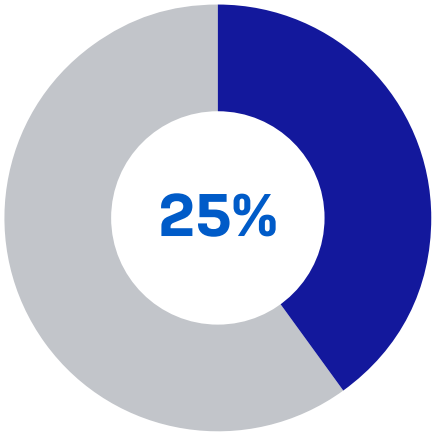
Devices are often not used for their original purposes

Not surprisingly, almost all consumers say their household uses a personal device for personal use. But for company-owned or school-issued devices, respondents were more likely to use them for purposes beyond just their intended ones – reflecting the likelihood that consumers will use any device that's convenient or available to them for online activity, and not necessarily restrict themselves to using specific devices for specific purposes.

For instance, more households use personal devices for school purposes than they use school-issued devices for school and homework.



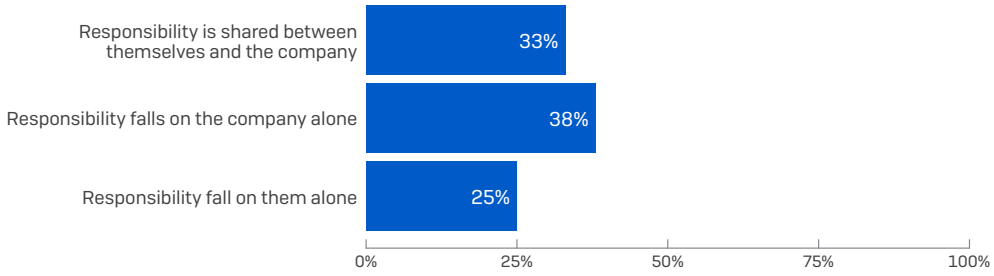
use a personal device for school/home work use



use a school-owned device for school/home work use

Security responsibility

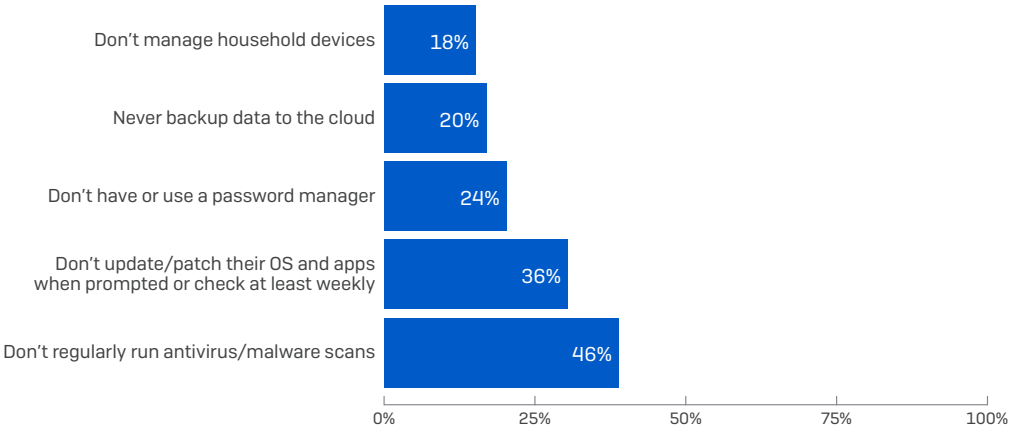
Consumers have mixed opinions on, and perceptions of, who is responsible for securing their company-owned devices.



Many consumers are not acting to protect themselves at all

Nearly one-quarter of consumers say they don't use password managers. Additionally, 20% of consumers don't back up data to the cloud.

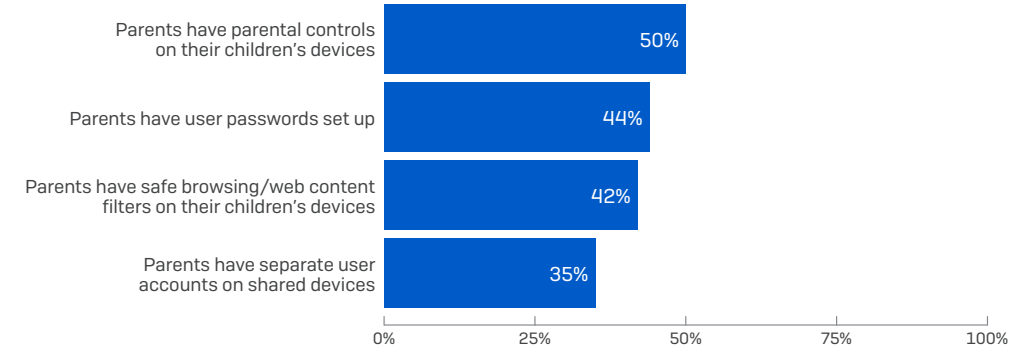
Nearly one-fifth of consumers say they spend no time managing household devices either, reflecting that no one within the household has any designated responsibility for ensuring devices are secure or updated.



Further vulnerabilities reveal themselves when looking strictly at respondents with children in the household.

Among parents, just 35% have set up separate user accounts on devices shared with their children and less than half have user passwords set up on these devices.

Additionally, only half of parents say they've implemented parental controls on devices their kids use and just over four in 10 say those devices use safe browsing or web content filters.

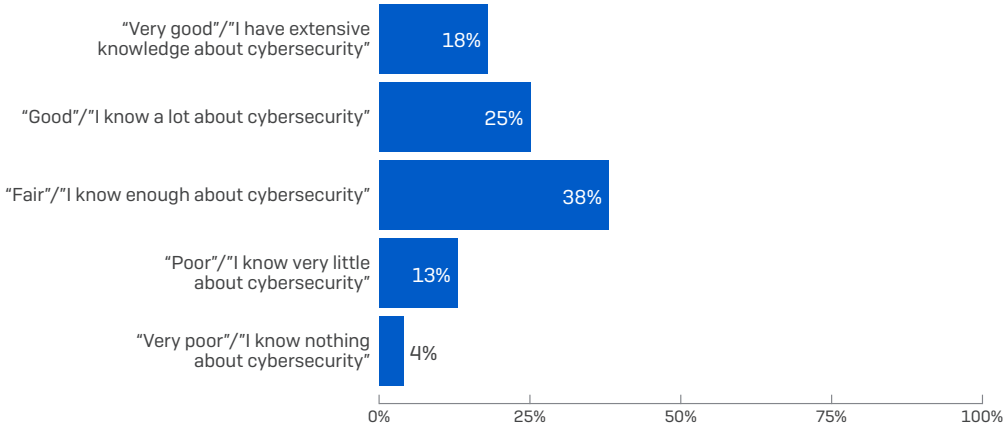


Part 3: Consumer security knowledge varies – for many, self-perceived levels of knowledge are inaccurately high

Consumers generally perceive themselves as knowledgeable about online security

More than four in 10 (43%) consumers surveyed professed to having "very good" or "good" knowledge about online security.

Nearly four in 10 others (38%) expressed having only a "fair" amount of online security knowledge, and almost two in 10 (18%) said they had poor or very poor online security knowledge.



Consumers' perceptions of their cybersecurity knowledge may be inaccurately high. As a result, their inaccurate understanding of cybersecurity could lead them to believing something that isn't true. For example, nearly a quarter of respondents (24%) falsely believe that Apple macOS is not affected by cyberattacks.

Most people believe that they understand ransomware; less than a majority actually do

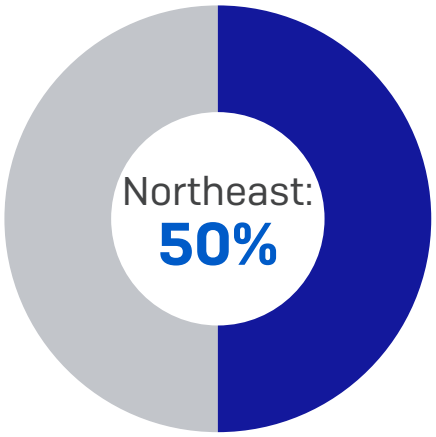
Among all respondents, a majority were unable to correctly identify ransomware, demonstrating a lack of security knowledge – even among those who say their security knowledge is "very good."

While 60% of all consumers claim to understand the term ransomware, only 49% among all respondents could correctly identify ransomware as "a malicious software designed to block access to a computer system until a sum of money is paid."

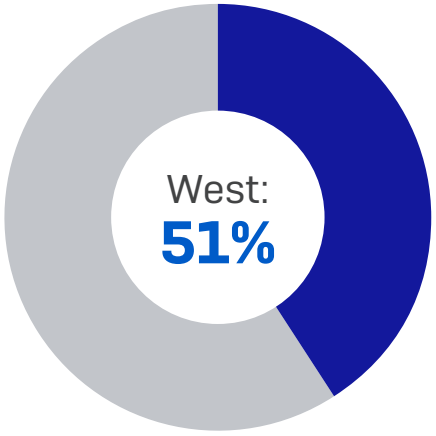
Among the full group of respondents, 36% attributed incorrect definitions to ransomware, while 15% didn't know at all.

Online security knowledge is the strongest among consumers aged 25-44 and those living in the Northeast

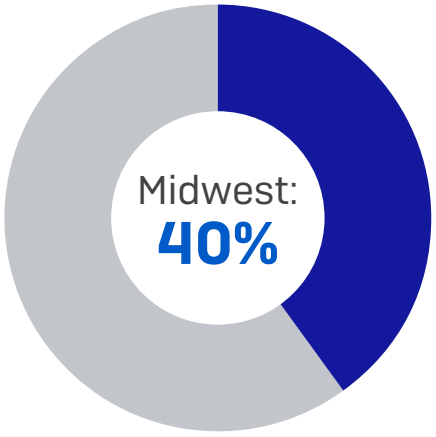
The Northeast is the only region where a majority of consumers say they have "good" or "very good" knowledge about online security. In the West and Midwest, nearly equal numbers of consumers say their knowledge is "good"/"very good." The South ranks the worst for cybersecurity knowledge, with 19% saying they "know little or nothing" about cybersecurity.



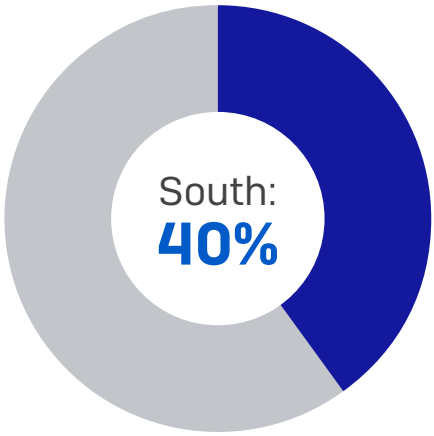
have "good"/"very good" security knowledge vs. 17% "little or nothing"



boast "good"/"very good" vs. 17% "little or nothing"



"good"/"very good" vs. 17% "little or nothing"

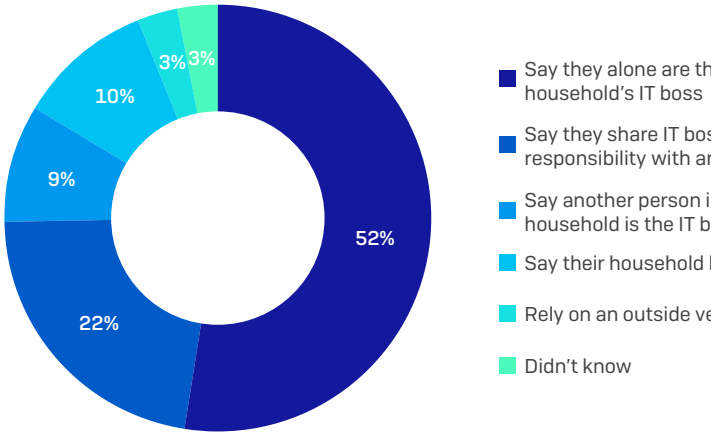


"good"/"very good" vs. 19% "little or nothing"

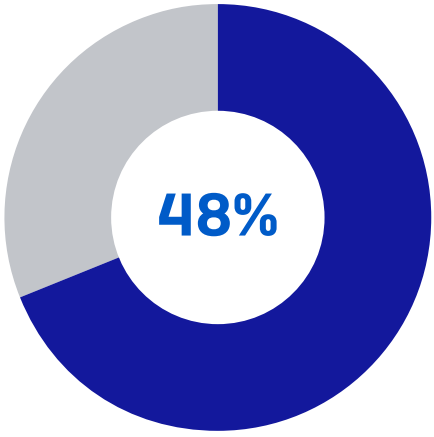
Among all respondents, 60% of those age 25-34 and 62% of those age 35-44 claim to have "good" and "very good" knowledge. Only 42% of those age 18-24 said the same. Among respondents 45 and older, just 38% believe they have "good" and "very good" online security knowledge.

Household IT responsibilities

More than eight out of 10 respondents (83%) say there is at least one person designated as their household's "IT boss" – the person designated to oversee and manage security for the household's devices. Only 10% of households have no IT boss.



Additionally, nearly half of respondents say they are also responsible for managing devices outside their household – e.g., devices belonging to parents, grandparents, on-campus college students, and other family and friends.



respondents manage devices outside their household

The Northeast is the only region where a majority (54%) of respondents said they manage devices outside their household. All other regions were below the majority line.

But while most households have an IT boss, there are still big gaps. Even among those who live by themselves, 12% are not managing their own IT security. Additionally, 30% of households with two to three people, and 24% of households with four or more people, do not have designated IT bosses.

While the number of households without IT bosses may be overall smaller, it points to a persistent lack of security oversight in many households.

Further Resources

Parents may find this blog post, 'Survey: Concerns about children's online security increase during a pandemic,' helpful as it focuses on data from this survey pertinent specifically to respondents with kids and school-related concerns, and provides specific recommendations to help parents better protect their children's online security.

These blog posts provide further clarity for debunking misconceptions and better safeguarding household online security:

- Work from Anywhere: Security Tips for Individuals
- Defining VPNs: Why Are They Important for Web Security?
- Are Macs Really Safer Against Cyberthreats?

Sophos Home provides security and privacy for the entire household, making it easy to secure and manage multiple devices. Users can easily manage Windows and Mac devices via a mobile app on their iOS and Android devices, no matter where they are or where extended family members live.

Learn how other households are using Sophos Home to protect their families.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

21-07-02 EN (DD)

SOPHOS