

2024 CONSUMER SECURITY SURVEY



It's no secret that our lives are powered by smart technology – from smart phones, watches, and TVs to the growing market of smart grills, mirrors, and glasses, smart devices are everywhere. While these add convenience to our lives, this influx of devices means increased risk when it comes to cybersecurity and data privacy. To understand how consumers are responding to this increase in security threats, the **2024 NETGEAR Consumer Security Survey** pulsed consumers on their cybersecurity habits at home, revealing some alarming data points about the impact of cybersecurity on home networks.

Despite research¹ finding that a home network sees an average of 10 attacks every 24 hours:



82% of consumers report they are confident that their home network is secure from external threats.



Nearly **one-third (30%)** of consumers report that cyberattacks against home networks are not common.

¹Source: NETGEAR & Bitdefender 2024 IoT Security Landscape Report



Increased cyber threats means there is a need for consumers to take proactive measures to protect themselves.

While some **(18%)** report taking daily precautions, nearly half **(44%)** are taking proactive measures on a bi-monthly basis or less, with **12%** responding they never take steps to secure their home network.

Weak password practices are also contributing to growing security concerns.

40% of people report having the same password across at least two of their accounts, while **more than one in four** report that they use the same password for 6 or more accounts!



Unfortunately, cyberattacks are a reality.



One in ten **(11%)** report that they have experienced a cybersecurity breach on their network in the last 12 months.

Of those that indicated they experienced a breach, they had varying consequences, including:



11%

Being locked out of a home network or unable to use devices



18%

Personal data or identity theft



13%

Monetary amount stolen up to \$10k

For all respondents, whether they had experienced a cybersecurity breach or not, there were a handful of events they were concerned about as it relates to the security of their home network:



52%

Personal data or identity being stolen



20%

Connected devices unable to be used or unable to work from home



18%

Falling victim to a hack such as ransomware



10%

Foreign government data collection



The good news: network security doesn't have to be challenging.

Powered by state-of-the-art encryption protocols and advanced threat detection mechanisms, NETGEAR routers stand as the first line of defense against evolving cyber threats and include various security features. Further, **NETGEAR Armor** provides an added layer of protection for your home network and devices connected to it. Many of the latest **Nighthawk routers** and **Orbi mesh systems** come with either a 30-day trial or a free one-year subscription of the Armor service. Learn more about how NETGEAR can power and protect your home network [here](#).

2024 NETGEAR Consumer Router Security Survey Methodology

This CARAVAN survey was conducted by Big Village among a sample of 2,016 adults 18 years of age and older. The online omnibus study is conducted three times a week among a demographically representative U.S. sample of 1,000 adults 18 years of age and older. This survey was live on June 26-30, 2024.

Completed interviews are weighted by five variables: age, sex, geographic region, race and education to ensure reliable and accurate representation of the total U.S. population, 18 years of age and older. The raw data are weighted by a custom designed program which automatically develops a weighting factor for each respondent. Each respondent is assigned a single weight derived from the relationship between the actual proportion of the population based on U.S. Census data with its specific combination of age, sex, geographic characteristics, race and education and the proportion in the sample. Tabular results show both weighted and unweighted bases.

Respondents for this survey were selected from among those who have volunteered to participate in online surveys and polls. The data has been weighted to reflect the demographic composition of the 18+ population. All sample surveys and polls may be subject to multiple sources of error, including, but not limited to sampling error, coverage error, error associated with nonresponse, error associated with question wording and response options, and post-survey weighting and adjustments.