CHUBB®

Personal Risk Services

COVID-19 & Life Online: Americans' Evolving Cyber Risks

Chubb Personal Cyber Risk 2021 Survey Executive Summary Report

COVID-19 has fundamentally reshaped every aspect of our lives, from where we work to who we see to when we go out. But, in the past year, one of the most understated yet outsized impacts of the pandemic have been on our cyber exposure.

According to the results of Chubb's fourth annual Personal Cyber Risk Survey, changes brought about by the pandemic—including widespread work-from-home—have exacerbated cyber risks for individuals and brought new consumer attention to cyber security. In fact, more than two-thirds (68%) of respondents report that they have become somewhat or much more concerned about the potential for a cyber breach exposing their personal information or identity in the past year. Compounding concerns is that with more information online than ever before, cyber bad actors have not just become stealthier, but also more vicious in how they attack personal data. Unfortunately, survey results show that despite more awareness of cyber concerns, we haven't yet matched this progress with risk mitigation action.

This report examines Americans' new cyber exposures, their comprehension of cyber risks, the steps they are taking to protect themselves, and where any gaps still exist. Read on for additional information and further details from Chubb's 2021 Personal Cyber Report.

86%

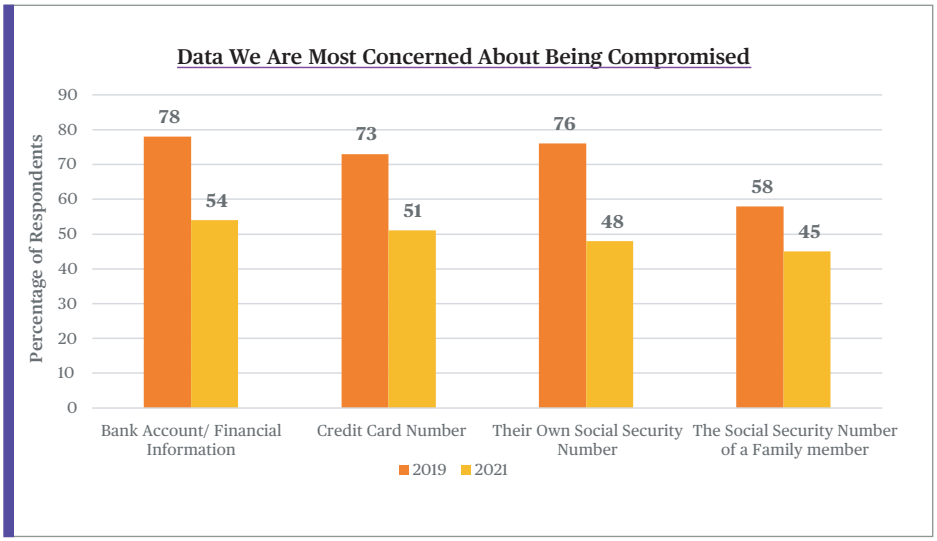
of individuals have either purchased or been gifted a new device in the past year

New Risks, New Ideas... Same Actions

In the past year, the COVID-19 pandemic has exacerbated cyber risks for individuals. In many ways, it has simply become a numbers game. According to the survey, 86% of Americans have either purchased or been gifted a new electronic device in the past year. Of those who did obtain a new device, 66% percent got a smartphone, 58% a laptop and 46% a tablet. Regardless of the device, if owners did not properly secure them in a timely manner, they could have exposed themselves to cyber threats.

More connected devices naturally mean more time spent online. In fact, 83% of respondents access the internet several times a day, and 30% estimate they share their data at least 10 times a day. Further, 35% of high-net-worth (HNW) individuals estimate they share their data more than 100 times a day. While these figures might not come as a surprise–we have all felt this abrupt transition to life online–spending more time "plugged-in" means we need to do a better job of understanding what data we are sharing and protecting the information we are releasing into the cyber universe.

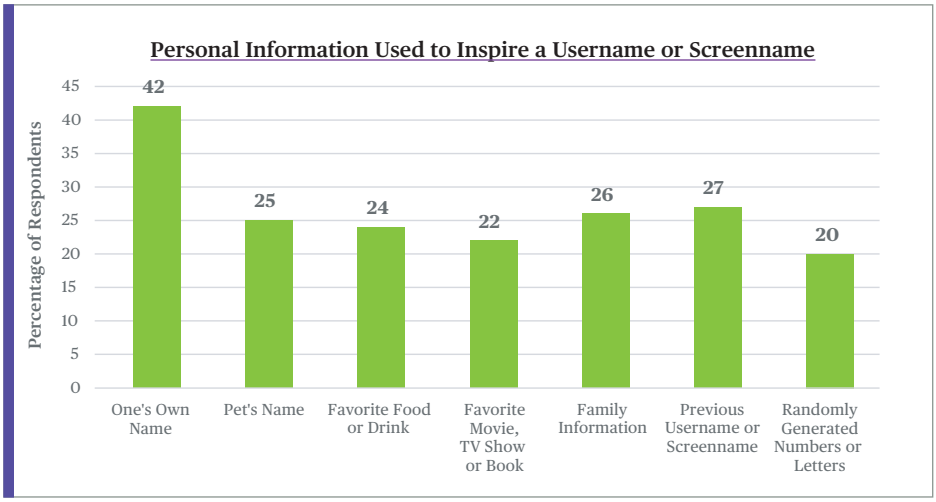
Unfortunately, findings from the survey show these behaviors are not practiced. When it comes to our understanding of our most vulnerable information, individuals are most concerned with financial information such as bank account (54%) and credit card numbers (51%) being compromised, followed by social security numbers (48%). Yet–when compared to Chubb's 2019 Cyber Survey–the overall level of concern surrounding these pieces of information has dropped. While the concern around social security numbers is a real one, banks and other financial institutions typically provide safeguards and extra layers of protection for financial information. Furthermore, credit card companies have made it virtually effortless to change your card number and re-secure your account. Many even offer fraud protection.



Where individuals actually should be most concerned is in other types of data that, much like a social security number, cannot be changed. This might include one's birthdate, but it also could include a variety of personal information, from pet names to favorite TV shows. The reason that personal data like one's birthdate is so sensitive is two-fold: it cannot be changed, and it is often "feeder information" that is used in various passwords/ access codes or in security questions to help users identify a forgotten password. For example, when creating screen names, (42%) of Americans draw inspiration from their own name and 57% of individuals report using personal information to inspire a password.

57%

of individuals report using personal information to inspire a password



Put simply, sharing personal information, no matter where, is dangerous–individuals tend to also use this information to build passwords, allowing bad actors to then guess log-in credentials to access accounts. To make matters worse, individuals tend to use the same passwords across multiple platforms. So, if a bad actor were to gain access to one, they may be able to grow the number of accounts they have access to quickly and easily.

Herein lies the greatest challenge: as individuals spend more time online and use personal information as their passwords, they are not taking the right preventative measures to protect themselves. In fact, the survey found that no more than a third of respondents report taking any preventative actions in the past year, including regularly changing online passwords (28%), no longer sharing passwords with others (18%), not using the same passwords for multiple accounts (22%) or using a personal VPN (17%). Not even the pandemic and its forced shift to more online interactions could change their ways, with the likelihood that respondents have taken these actions remaining steady pre- and post-pandemic–in 2019, 31% of respondents reported changing online passwords, versus 28% today.

Despite the fact that individuals are not taking action to protect themselves from cyber risks, they do feel confident they would know what to do if their personal information was compromised. The majority of individuals (85%) feel they either have a general idea or know exactly what to do if their personal information is compromised.

However, what most people don't account for in their response is the potential for significant legal, financial, and reputational ramifications of a cyber incident. These factors are particularly critical when it comes to the intersection of work and home life, a line that has only become blurrier in the past year. Now, clicking one malicious link on a personal device could also allow a bad actor to compromise your employer's data and information.

Whether working remotely, spending more time on social media, helping children learn remotely or catching up with friends, Americans understand that this increase in online activity has left them more vulnerable to cyber attacks. Many simply don't understand how easy the right actions are to take.

Cyber Misconceptions: In-Office Work & Social Media

When it comes to the actions individuals believe are the most vulnerable or most cyber secure, there are a few striking misconceptions:

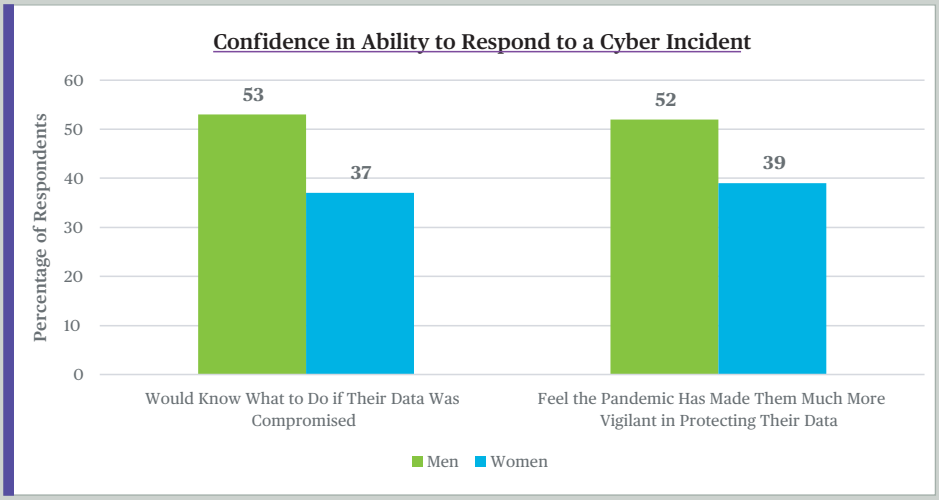
Working in the office ranked as more vulnerable to cyber attacks than working from home–22% of respondents ranked in-office work as most vulnerable, versus 11% of respondents who cited working from home as most vulnerable to cyber attacks. Unfortunately, this is not the case, as remote work comes with an increase in endpoint vulnerabilities and less company control over how secure individual employees are keeping their home networks.

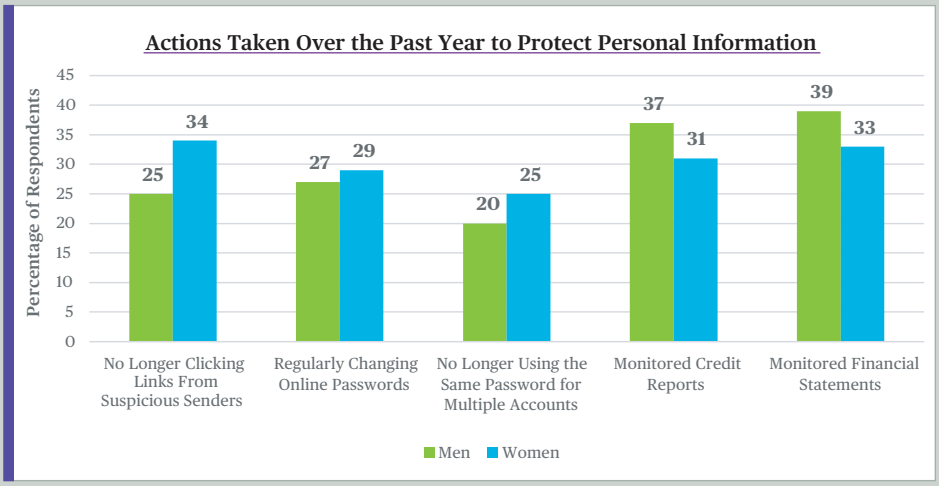
Social media is among what is thought to be most secure–27% of respondents ranked it among the most secure activities. But, again, this not the case. Social media can be especially dangerous from a cyber security perspective because individuals tend to overshare pieces of personal information that we cannot change, like one's name, birthdate, and pet's name. These tidbits, no matter how small, can then be pieced together by bad actors to guess passwords, gain access to your accounts, and steal even more information.

Men and Women Emphasize Cyber Security Differently

When it comes to cyber security attitudes and actions, the differences between men and women are striking: men are overall more concerned about cyber security risks. Men are also more confident in how they might respond if a cyber incident were to occur, and in their ability to take the right steps to prevent a cyber exposure.

However, confidence doesn't always mean someone is right. According to the survey, women were more likely to take the necessary steps to protect their personal data, whereas men focus largely on protecting financial information–information that is already fairly secure and easily recoverable.





44%

of individuals chose to relocate to work remotely during the COVID-19 pandemic

We're Too "Cyber Comfortable" at Home

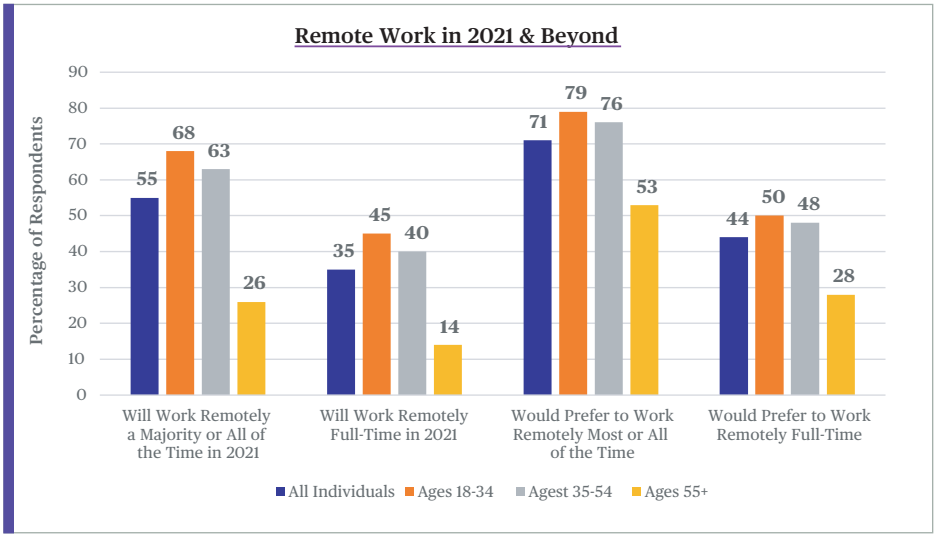
While many people didn't have a choice of where to work during the pandemic, some individuals were able to relocate to the remote location of their choosing, whether a second home or short-term rental. Specifically, 44% of individuals chose to relocate to work remotely during the COVID-19 pandemic. Overall younger groups and those with the means to do so more often made this move:

- 56% of individuals age 18-34
- 51% of those age 35-54
- 59% of high-net-worth individuals

No matter where they were working, remote work comes with additional endpoint cyber vulnerabilities. These vulnerabilities only grow when you add additional location changes to the mix–as one might have holed up in a secondary home with out-of-date security software, or a temporary rental with a public Wi-Fi network.

For most Americans, "home" is synonymous with safety and comfort–as such we have a tendency to relax and let our guards down when in our own homes. The same, it turns out, is true when it comes to our cyber security behaviors and practices. On the other hand, of the individuals who escaped cramped quarters and relocated either temporarily or semi-permanently to another remote working location, many took the right steps to protect themselves and both their personal and company data. Notably, of those who moved, 62% of respondents changed passwords, 43% used a VPN even on a private network, and 43% made sure to log out of all accounts when transitioning to and from their temporary locations. While most individuals have not regularly practiced these same "best cyber behaviors" in their day-to-day lives, individuals do see the connection between physical location changes and needing to take precautionary measures.

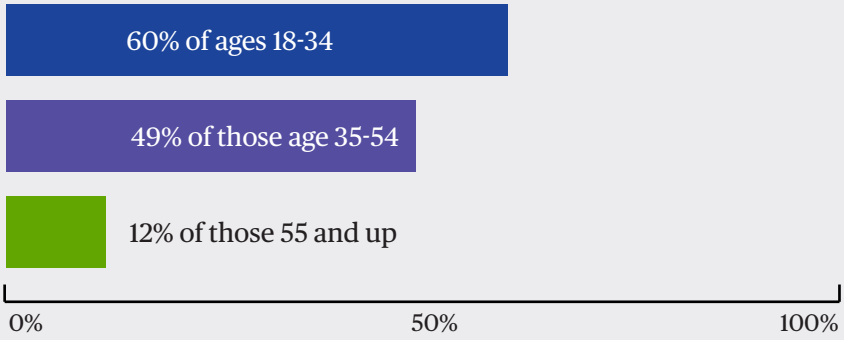
Looking ahead, with a majority of Americans anticipating they will work remotely most or all of this year (2021), companies should remain vigilant when it comes to employee security best practices.



Of all employees, younger groups have enjoyed the freedom of remote work much more than their older colleagues. In order to appeal to and retain younger talent, some companies may look to be more accommodating to their remote working preferences. Thus, instilling cyber security best practices now is critical to ensuring the long-term security of their businesses, as remote work appears to be here to stay.

The Rebirth of the Entrepreneur

Younger generations have more faith in the ability of small businesses to protect themselves and their customers against cyber attacks, while their older counterparts remain skeptical. When asked whether small businesses are as prepared to protect consumer information as larger companies, the following agreed:



Aside from a generational difference, this could be due in part to the spike in entrepreneurism in light of the COVID-19 pandemic—many younger adults are choosing to set off on their own and start small businesses in order to reclaim control over their lives and schedules.

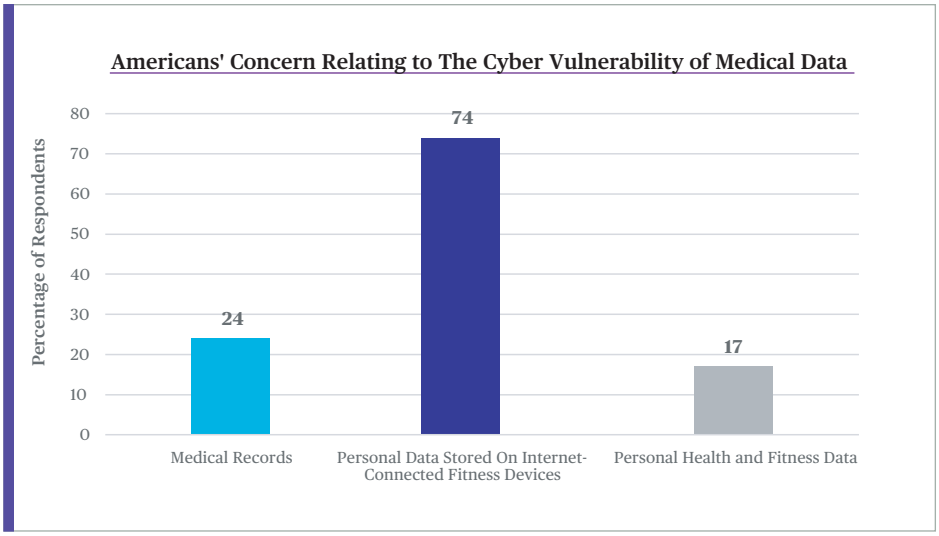
But whether brand new or more established, small businesses are frequently the target of cyber attacks. In fact, the Chubb Cyber Index®, a proprietary database of more than two decades of claims data, shows that, since 2012, global cyber incidents have grown by 981% for small businesses with revenues under $25M. This is because bad actors have had success in targeting small businesses, as these smaller companies may have fewer resources to put protections in place. As a result, small businesses should be as, if not more, vigilant than larger companies when it comes to their cyber risks.

Medical Data Vulnerabilities Go Unnoticed

Our medical information has become more top-of-mind and conversations around health more commonplace in the past year, especially as it relates to the COVID-19 vaccine.

According to the study, most individuals (63%) feel as though others should share their vaccination status in order to be able to participate in normal activities, but a similar majority (57%) are concerned with having to share their vaccination status with others. This suggests an interesting disconnect: Americans understand the importance of vaccinations and transparency to help us all return to normal again, but also have lingering concerns about privacy relating to this personal information.

While respondents expressed concern about privacy as it relates to vaccination status, the same level of concern does not extend to other sources of medical data, with the notable exception of fitness tracking devices.



This lack of concern is alarming as medical records are extremely sensitive and, if they fall into the wrong hands, can be a challenging issue to remedy. For example, patient medical records contain the individuals' full name, address history, financial information and often social security number–which is more than enough information to allow bad actors to impersonate a patient to get medical services, open a line of credit, break into bank accounts, or even illegally obtain drugs so that a patient cannot fill (or has to pay out-of-pocket) for their prescription.

Even the world's greatest public health crisis of the last century has not altered concern. Looking back to 2019, a mere 27% of respondents were concerned with their medical records falling into the wrong hands. Despite the world's eyes on our health data during a global pandemic, the overarching data vulnerability concerns around our medical information have remained flat year-over-year.

A similar disparity is present among Internet of Things (IoT) connected fitness devices and the personal health and fitness data stored within them. Most individuals are concerned about the security of their personal information (name, age, birthdate, etc.) on a fitness device (74%). But relatively few respondents (17%) expressed concern about their personal health and fitness data (heart rate, fitness levels, workout habits, etc.) being compromised. While Americans understand that cyber security is something to be concerned about, they may not be seeing the whole picture when it comes to the universe of our data vulnerabilities–particularly, that both personal ***and*** health data are critically important to protect.

Is It a Love Connection, or Are They Just Pining After Your Data?

When it comes to online dating apps, many are looking for love. But some are just looking for your data.

Whether they ask you to send them money or are all too eager to inquire about personal information, online dating scams can take a number of different forms. In fact, according to the Federal Trade Commission, reports of these online scams have nearly tripled in the past few years, and in 2019 alone victims lost around $201 million being swindled by a cyber sweetheart.

At the same time, it turns out most people still believe what they see on dating apps is what they'll get. In fact, 64% of survey respondents believe people are very or somewhat truthful with the information they share on online dating sites. When it comes to finding a potential match, men appear to be slightly more trusting than women, with 38% of men believing people are being very truthful with their profiles, versus just 22% of women.

But just because people are more trusting in their quest for love doesn't mean they are unaware of privacy concerns. The vast majority of individuals–85% to be exact–remain somewhat or very concerned with their personal information being shared with others on an online dating site. But that doesn't mean usage of these sites has gone down. While individuals might recognize the risks of telling a stranger their birthdate, they still do so. In the quest for love, as it turns out, cyber security has taken a backseat.

Americans Stick to What They Know When It Comes to Cyber Insurance

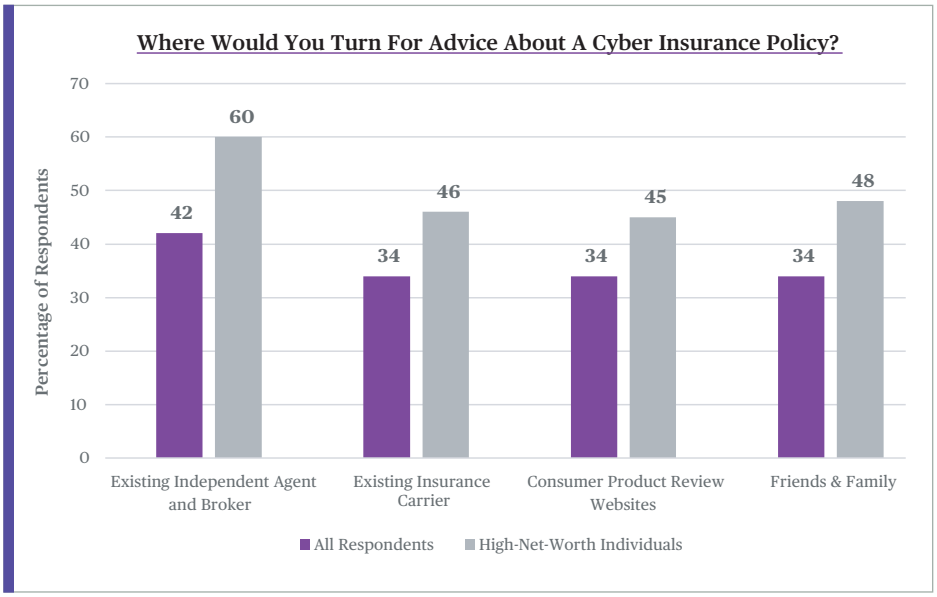
Despite broad exposure, only 12% of Americans have purchased a personal cyber insurance policy in the past year. This small group of Americans has recognized their need and taken steps to fill a gap in their insurance coverage. More could benefit from following their lead.

For others who are still considering making a purchase, these individuals are most likely to rely on a trusted source like an insurance agent, existing insurance carrier or family member/friend to direct them towards the best policy for their unique needs.

Ultimately, when it comes to making insurance purchasing decisions–and understanding that everyone's needs are different–individuals prefer to lean on people who know them and who they trust. For a majority of consumers (70%), that includes preferring to purchase their cyber insurance policy through their existing carrier.

It also suggests that consumers prefer to work with a holistic insurer so that they have the option to add additional specialized offerings–cyber or otherwise–when the time and need arises. Working with a single carrier can also help optimize cost.

For more information about personal cyber security exposures, resources to safeguard you and your loved ones and how a cyber insurance policy works, visit https://www.chubb.com/us-en/individuals-families/



Methodology:

This is the fourth survey by Chubb measuring consumers' approaches and behaviors toward cyber risk. Conducted by Dynata, , a leading global provider of first-party consumer and professional data, the online survey was fielded between February 11-25, 2021. The results are based on 1,208 completed surveys. A breakdown of respondents is as follows:

- **Gender:** Male (53%), Female (46%), Non-binary/ Prefer Not to Answer (1%)
- **Age:** 18-34 (36%), 35-54 (40%), 55+ (24%)
- **Regions:** Midwest (19%), Northeast (21%), West (27%), South (32%)
- **Socioeconomic Status:** Middle Class (27%), Upper Middle Class (27%), Mass Affluent (24%), High-Net-Worth (22%)

CHUBB®

Cyber Best Practices Cheat Sheet

Taking the right steps to protect your personal data doesn't have to be a hard or daunting task. By following the below guide, we can all get most of the way to being cyber secure:

1. Keep your software up-to-date

- Use anti-virus protection and cyber security software
- Install software and app updates ("patches") as soon as possible, or turn on automatic updates

2. Change your passwords regularly and always use strong passwords

- Do not share your passwords with others
- Do not use the same password for multiple accounts
- Use a password manager app

3. Manage your credit profile

- Review your credit report periodically
- Sign-up for credit monitoring service
- Freeze your credit with all 3 bureaus

4. Manage your data

- Don't store compromising electronic data about yourself that someone could use against you
- Back-up data you can't afford to lose both in the cloud and on an offline storage device (like an external hard drive)

5. Use multi-factor authentication to log into accounts

6. Use a personal VPN, even on a private network

7. Be wary of social media

- Don't accept social media "friend" requests from strangers
- Don't share sensitive or personal information on social media

8. Watch what you click

- Don't click links from unknown or suspicious senders
- Don't click sale or digital coupon links in emails

Chubb. Insured.[SM]