

5732C20C10  
076C6200  
00200C697  
0A16C20Data  
02E6E01000  
0E6E010008b  
Cyber Attac  
06564207360  
06564207360  
C6E2074686  
0360A000100  
0360A000100  
0AFFA33C08E0  
02073 0732C2  
02073 0732C2  
6E642001A!D  
0E6E01000

Fall 2024

---

Carat Insights

# Table of contents

- 03 Introduction
- 05 Cybersecurity in everyday life
- 08 Human error is leading cybersecurity concerns
- 10 Assessing the digital marketplace
- 12 Security vs. convenience
- 14 The rise of fraudulent practices
- 16 AI and the digital economy





# How consumers proactively face modern-day cybersecurity challenges

The cybersecurity and fraud landscape has dramatically shifted over the last few years, as the exponential growth of the digital marketplace has, consequently, ushered in opportunities for bad actors to exploit the space. The result is a new reality where large-scale data breaches and fraud are no longer a matter of “if,” but “when.”

In fact, consumers in recent years have seen even the biggest organizations succumb to cyberattacks. More than 90% of LinkedIn’s user database ended up on the dark web in 2021<sup>1</sup>,

while Facebook also announced the exposure of 530 million-plus account records that same year<sup>2</sup>. More recently, Roku announced more than half a million accounts were breached, with almost 400 users’ information exploited to make purchases<sup>3</sup>.

As the public has become more aware of ever-present cybersecurity threats, another interesting trend has emerged.

Consumers feel increasingly empowered to take a proactive role in their cybersecurity practices, especially as it pertains to their financial information.

The Fall 2024 Carat Insights report dives into how consumers react to cyber-insecurity and fraud threats, and what merchants can do to protect their customers by helping to put their minds at ease when shopping online.

The study pulls findings from a quantitative study of 1,000 U.S. consumers, with additional insights provided from interviews with a dozen CISOs from national organizations.

<sup>1</sup> Forbes: Details On 700 Million LinkedIn Users For Sale On Notorious Hacking Forum, June 29, 2021

<sup>2</sup> WIRED: What Really Caused Facebook's 500M-User Data Leak, April 6, 2021

<sup>3</sup> CBS News: Roku says 576,000 streaming accounts compromised in recent security breach, April 12, 2024

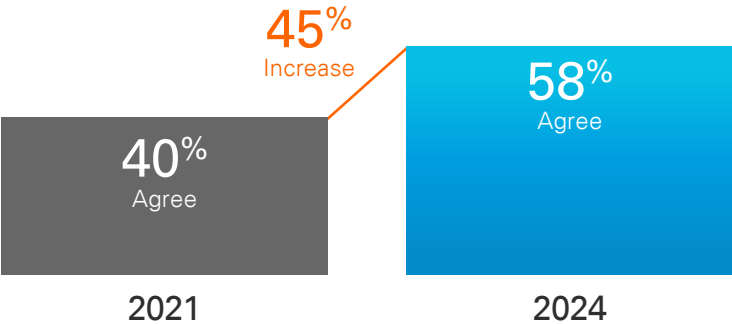


# Cybersecurity in everyday life

## Cybercrime is the expectation, not the exception

Hacks. The dark web. Identity theft. Phishing. Sadly, these terms have become a part of consumers' vernacular as cybercrime is now an unwelcome part of everyday society.

### Cybercrime is inevitable in our society



While two-thirds have experienced a cyberattack, attempt or threat in the last 12 months, consumers overall are generally less concerned about cybersecurity. In fact, nearly 1 in 5 say they are less concerned about cybersecurity today, compared to only 1 in 10 in 2021.

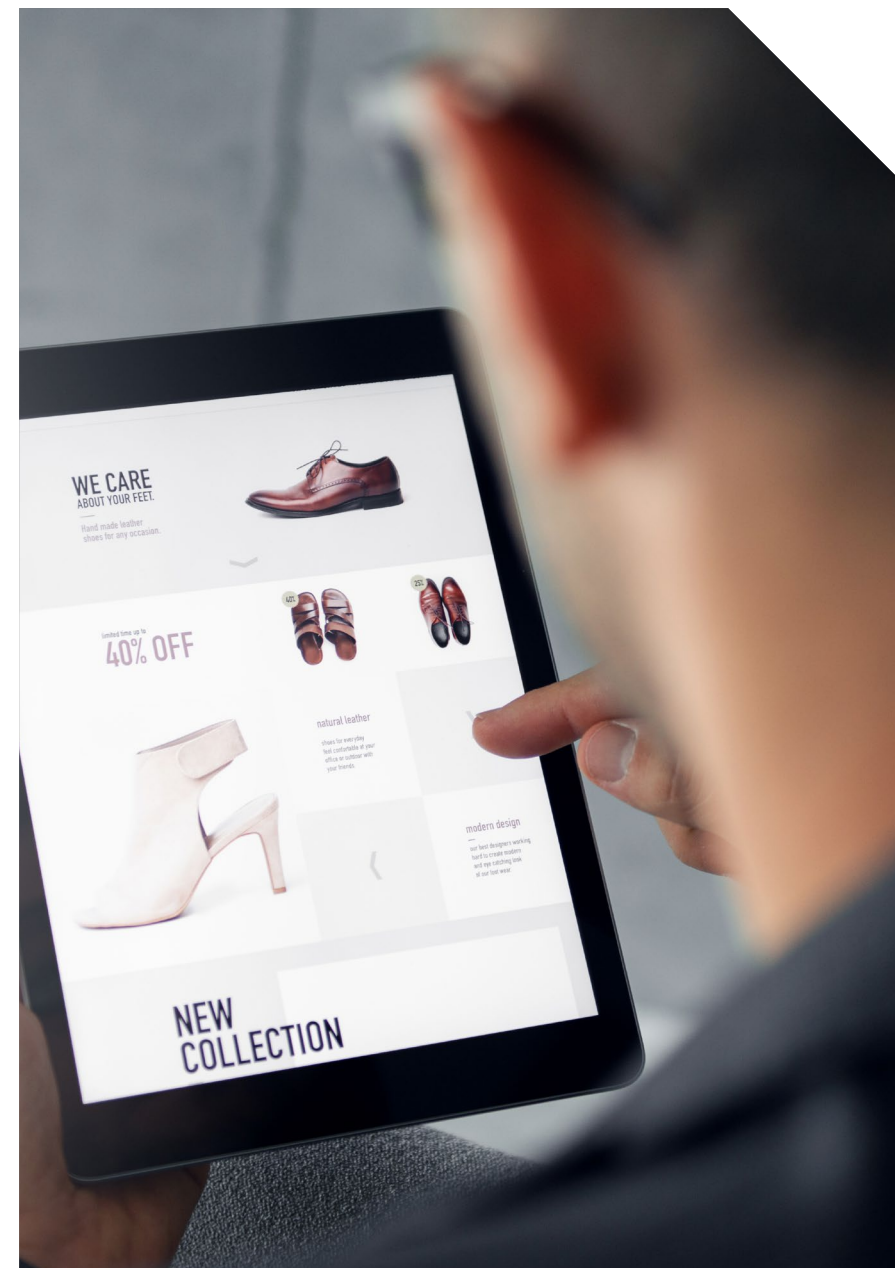
This general acceptance of cyberattacks creates its share of concerns for information security executives, who have mixed thoughts on how this shifting consumer mentality will impact the future of cybersecurity.

For example, as one global utility Chief Information Security Officer remarked, general acceptance is dangerous. An attacks-are-inevitable mindset could put a lot of consumers and businesses in a position in which they pay less attention to security.

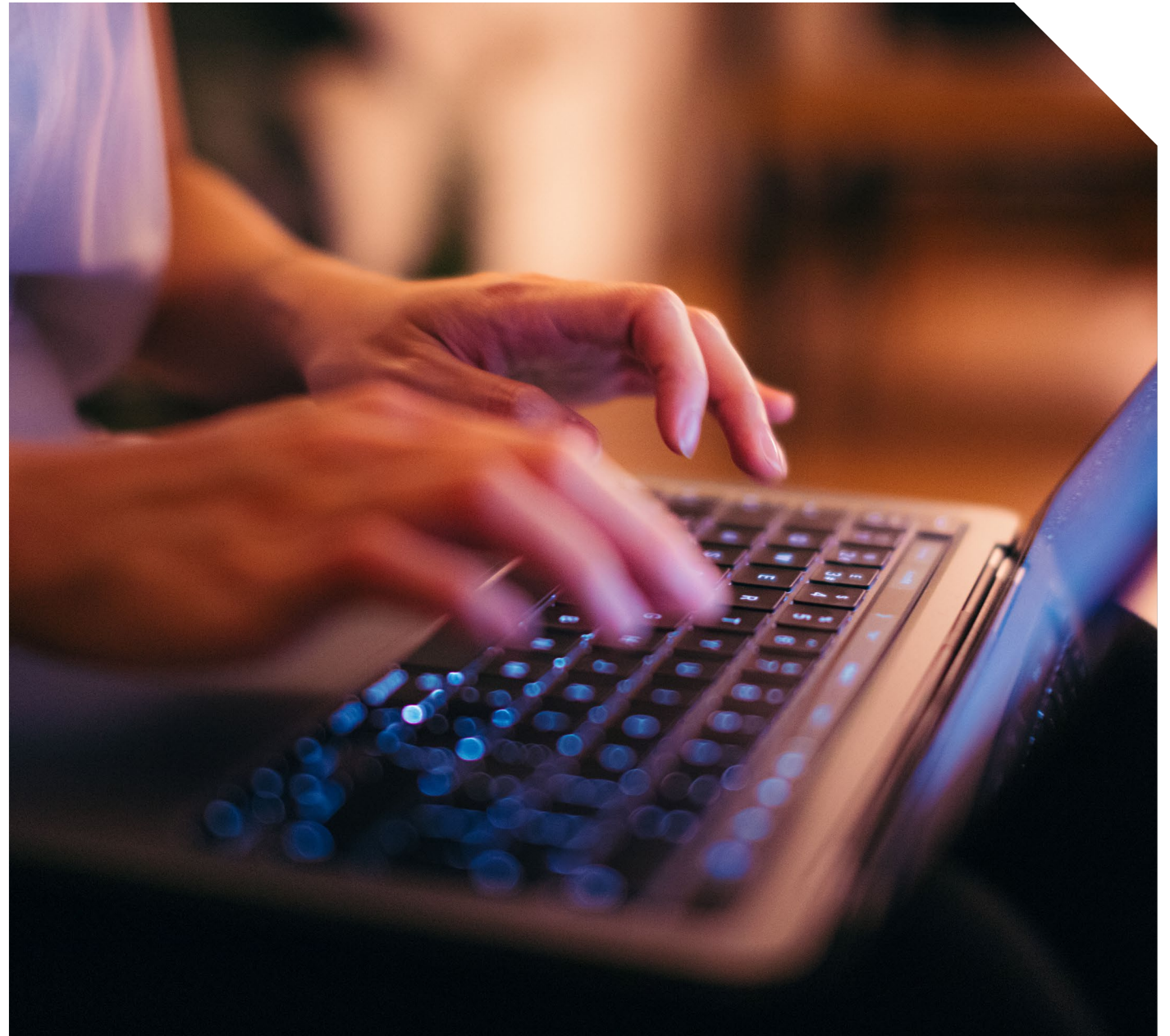
Other CISOs are more optimistic, with many noting that the prevalence of cyberattacks is empowering consumers to take security seriously.

According to a leading global insurance CISO, “[Cybersecurity] is not just a hassle anymore, [consumers] recognize that this is something we’re investing in to help protect them.” Likewise, a banking CISO commented on how “the executive community at the CISO level are more prepared today than they were 10 years ago [to handle a cyber incident].”

As noted by practitioners, the rise in cybersecurity incidents brings new opportunities for merchants. Consumers realize it’s inevitable to share their data in exchange for convenience, so merchants must create a safe environment for them by enacting measures to protect their information. Further, merchants should communicate with customers on any security changes to ensure peace of mind.



## Growth in cybersecurity issues since 2021

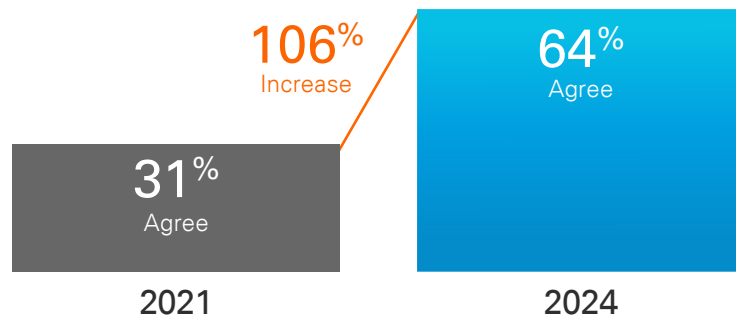


# Human error is leading cybersecurity concerns

For consumers, the human factor has overtaken technology

In the last three years, consumers have flipped the script regarding who's to blame for cybersecurity breaches, placing human error ahead of technology.

**The majority of cybersecurity breaches are the result of human/consumer negligence, rather than a technology failure.**





Consumers increasingly recognize human error in cybersecurity breaches, and as a result, more people are proactively introducing security measures. This includes opting into two-factor authentication (72%), changing passwords (65%) and relying on a password manager (51%) to keep their personal info safe.

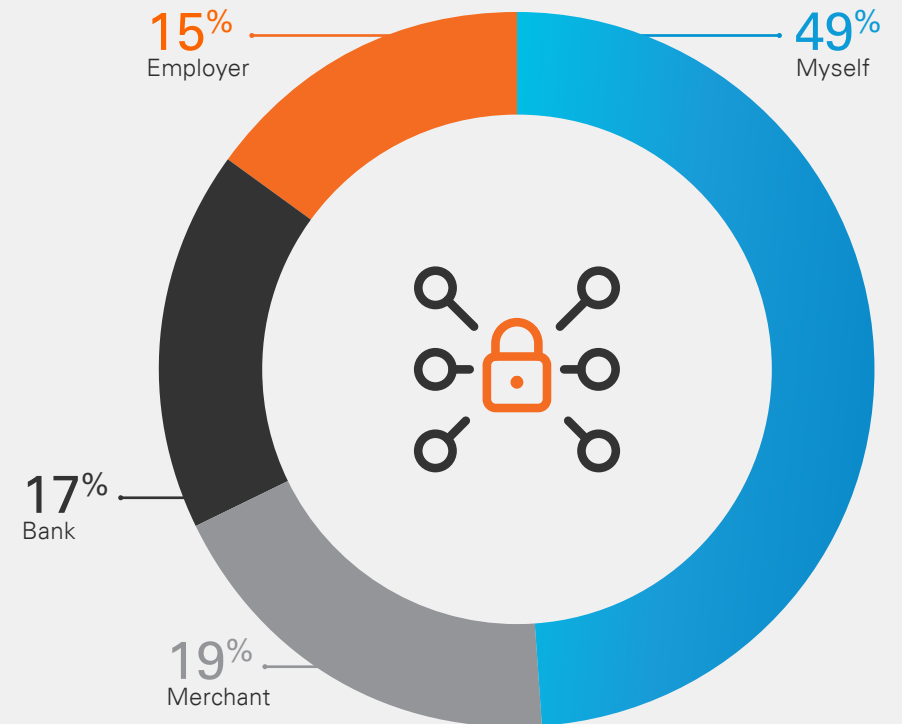
At the same time, consumers understand the difficulties that come with the added responsibility of protecting their sensitive information. Nearly one-third (32%) say it's too complicated and time-consuming to take all necessary precautions to protect their personal information. This number has risen as the cyber landscape has grown more complex, increasing from 18% in 2021.

These findings suggest businesses should offer tools and solutions to increase security across the board. According to CISOs, this is accomplished in two ways.

First is through ongoing training, suggested by 4/5 CISOs. As consumers place the burden of responsibility on themselves, merchants can lean into this consumer sentiment through ongoing training. This can include providing access to resources as well as in-app or browser education. Training, in whatever form it comes, is going to continue to raise awareness and create a sense of security among consumers.

Second, CISOs emphasize the importance of direct communication – and, often, overcommunication. This includes detailing how a particular merchant will communicate with consumers (for example, how Amazon will never call or text a customer about a suspicious purchase) as well as implementing communications to warn consumers about potential fraudulent actions before they take them, whether through alerts or notifications.

### Who is most responsible for ensuring I am protected from cybersecurity attacks?



# Assessing the digital marketplace

Despite the convenience, consumers show mixed feelings around the digital payments ecosystem

Accustomed to doing things remotely, consumers are increasingly reliant upon the digital marketplace. Despite growing usage, security concerns remain, which creates opportunities for organizations to stand out from the crowd. The more steps merchants take, the better.



55%

of consumers make at least 50% of their purchases online



75%

trust the physical payments ecosystem over the digital one



Although 55% of consumers make at least 50% of their purchases online, many are still hesitant about the digital marketplace. In fact, three in four consumers trust the physical ecosystem more than digital one.

At the heart of this concern is the ongoing struggle between convenience and security. As stated by a leading bank CISO, “If it’s too complicated, they’re not going to do it. Ultimately, convenience is king.”

Further complicating the matter is the crossover between consumers’ preferred online shopping payment methods and the methods they feel are least secure. Specifically, most consumers are using credit cards (32%), digital wallets (27%) and debit cards (20%) online, all of which are among those found to be least secure. Digital wallets are deemed the least secure by 36% of consumers, followed by debit cards and credit cards at 35% each.

One way consumers can protect themselves is by using reliable business and payment apps. “Not every digital wallet out there is going to have the same pedigree,” a banking

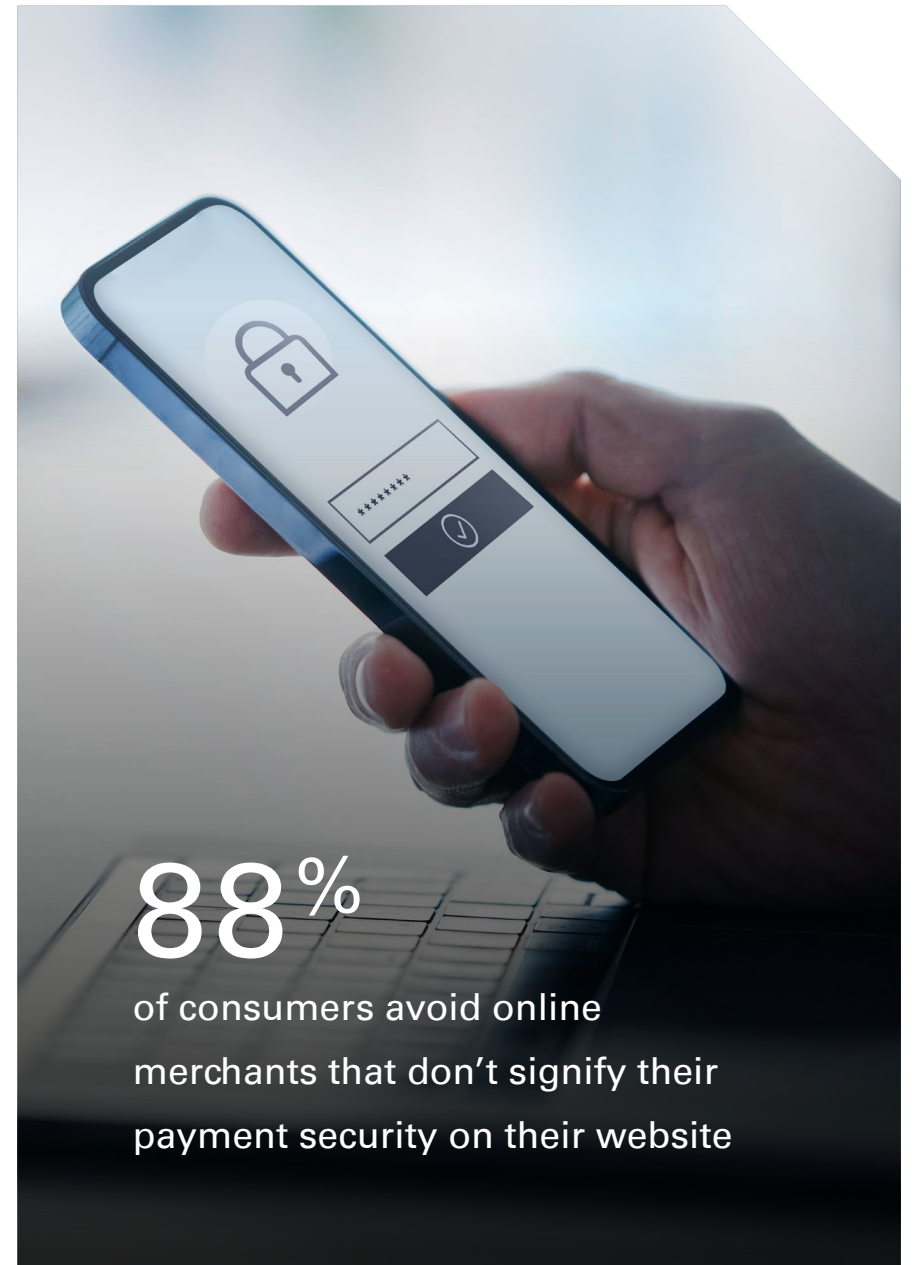
cybersecurity executive said. “When your money is at stake, it’s important that you make sure you’re using reputable vendors.”

Merchants can also put customers at ease by incorporating advanced security functionalities to their marketplaces.

For example, they can offer:

**Virtual Card Payments** – Nearly nine in ten (88%) consumers are likely to use a virtual credit card to protect their sensitive information if offered by a merchant. CISOs note how this approach adds an extra layer of security without inconveniencing consumers.

**Guest Checkout Capabilities** – Saving payment methods is an area of consumer apprehension, as 82% feel the presence of pre-populated payment information jeopardizes security. That’s why 42% of consumers will check out as a guest when the option is available.

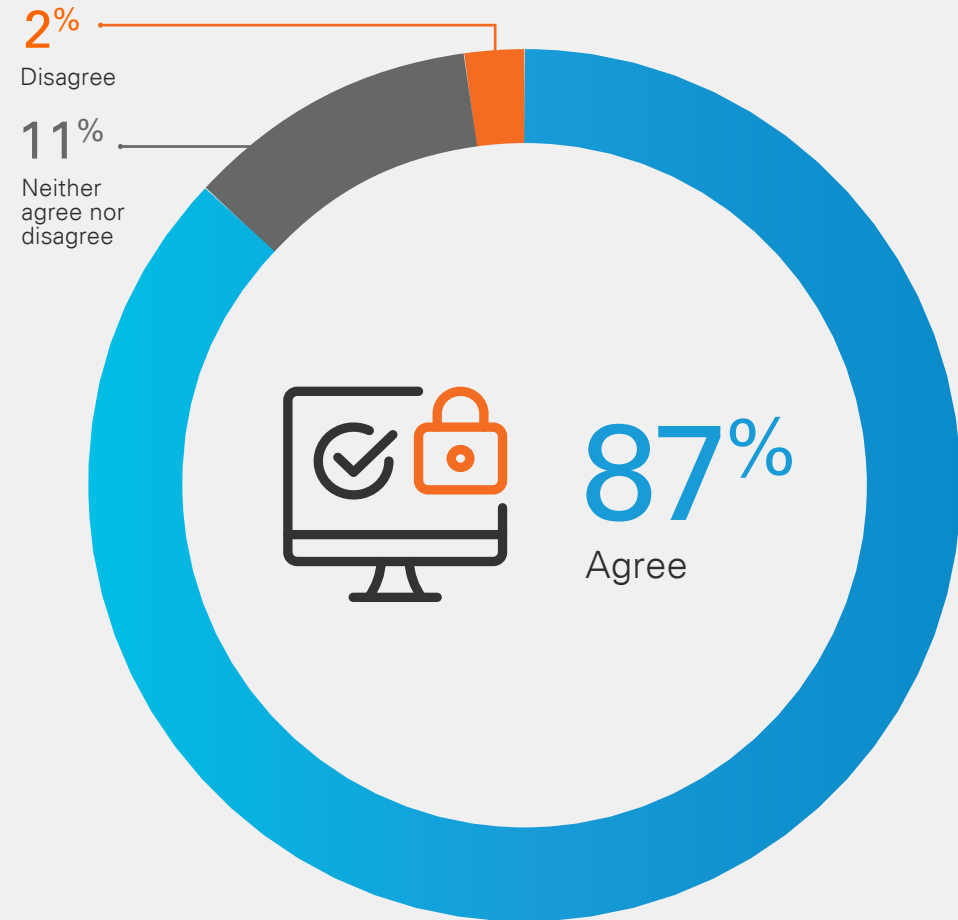



# Consumers weigh security vs. convenience

## MFA offers both peace of mind and frustrations to consumers

Although consumers overwhelmingly agree that multifactor authentication (MFA) practices help protect them, they are also frustrated by the inconvenience. Merchants should explore MFA practices that provide security while creating a seamless experience.

**MFA practices make me confident that my transaction is secure:**





“We need to be listening to the customers and the business and enable each to do what they want in a secure and realistic way.”

— Retail CISO

Consumers are quick to recognize the benefits MFA brings to their overall security. Specifically, 87% believe it makes transactions more secure and 72% use the process to protect themselves. While they can't argue with the benefits, consumers are quick to call out the friction MFA brings to the purchasing process. Specifically, 67% have abandoned a purchase because of excessive authentication requirements, and 57% agree with the statement “MFA practices cause more friction than peace of mind.”

These views play into the challenge of maintaining a balance between security and convenience facing businesses.

As noted by one cybersecurity executive, “the convenience we want must be supported by the security we need.”

Merchants should explore step-up authentication, recommended by nearly a third of CISOs. Many cite the complications that arise by placing too much friction too soon, which can alienate even the most avid users. Merchants should determine their higher-risk activities and consider only applying added protection to those events. For example, think about additional security measures for anything that involves a purchase or transfer of funds.

Likewise, it's important to embrace more seamless authentication methods.

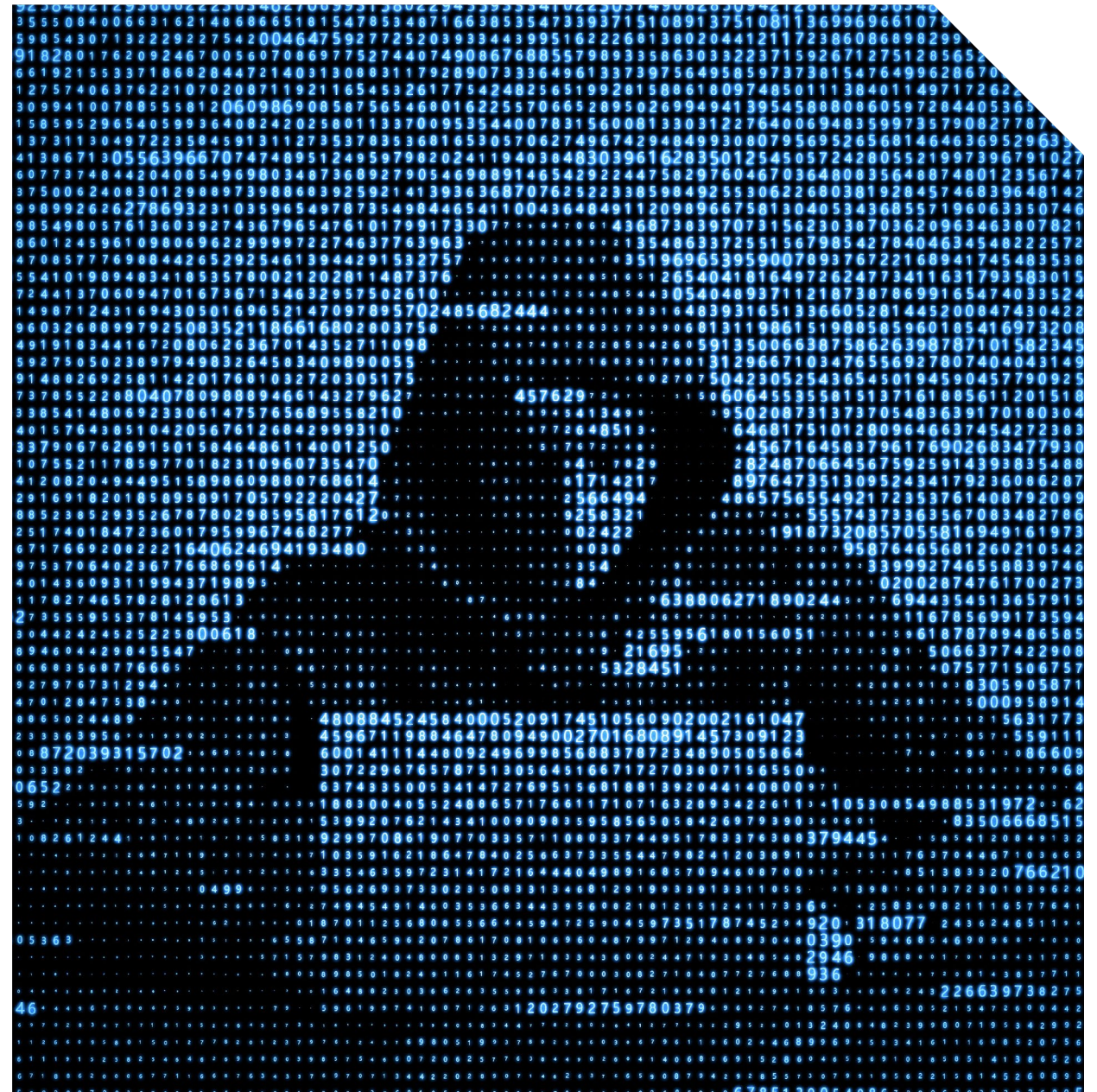
CISOs note the prevalence of mobile-based MFA processes, including text codes and facial and fingerprint recognition as a means of striking the balance between MFA frustrations and security. Consumers seem to follow this thinking as well, as text codes (73%), email codes (56%), facial recognition (53%) and fingerprint recognition (46%) are all preferred over traditional security questions (39%).

# The rise of fraudulent practices

Account takeover remains a top concern for consumers, but there is more they can do to protect themselves

Most consumers fear having their accounts jeopardized and actively work to protect their information. At the same time, despite their efforts to protect their accounts from being compromised, consumers also exhibit behaviors that further contribute to the growth of fraud.

## Consumers' complicated relationship with fraud



In today's marketplace where everything from retail purchases to reading news requires an account, consumer data is more at risk than ever. It comes as no surprise then that 80% of consumers are worried about account takeover fraud.

The rise of subscription services has led many to take actions that may contribute to the problem, as 48% admit to actively sharing account usernames and passwords with others. Among the most shared are television streaming services (80%), music subscriptions (66%) and news subscriptions (64%).

While account takeover is at the top of consumer lists, it isn't their only fraud-related fear. Concerns around phishing (53%), social engineering (44%), payment fraud (37%) and password attacks (35%) round out their top five.

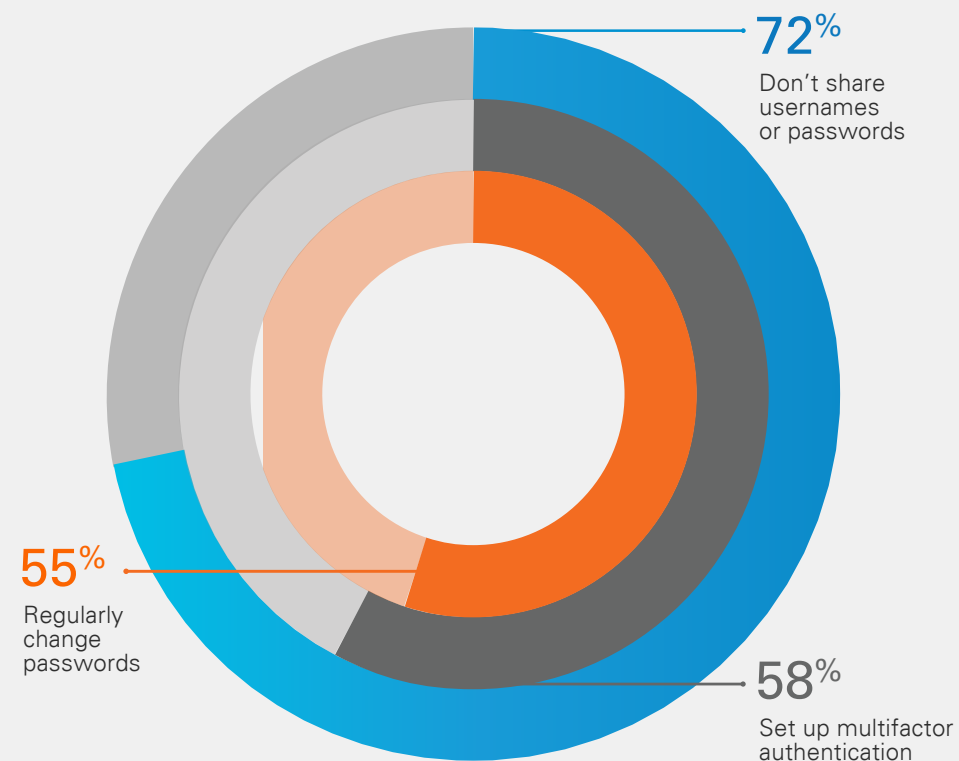
Additionally, consumers, whether knowingly or unknowingly, are committing first-party fraud. Nearly two-thirds (63%) of them have disputed a transaction for an online order without returning the item. Further, 62% have called their bank or card provider and asked for a refund on a subscription they forgot they had in the first place.

It's important for businesses to protect themselves as well as consumers. Education and training are key for both, but many merchants are also exploring more proactive measures aimed at reducing fraudulent practices. These include limiting customer logins to reduce password sharing and exploring transaction monitoring tools.

"We need to do things like leverage new technologies to look for inconsistent consumer patterns related to specific accounts," states a financial CISO. Such practices, she says, can help reduce fraudulent habits for both parties.

Other CISOs note the importance of these intelligence tools to ensure that consumers' legitimate orders are approved, while those seeming to abuse the system are tagged and vetted.

### How consumers protect themselves from an account takeover:

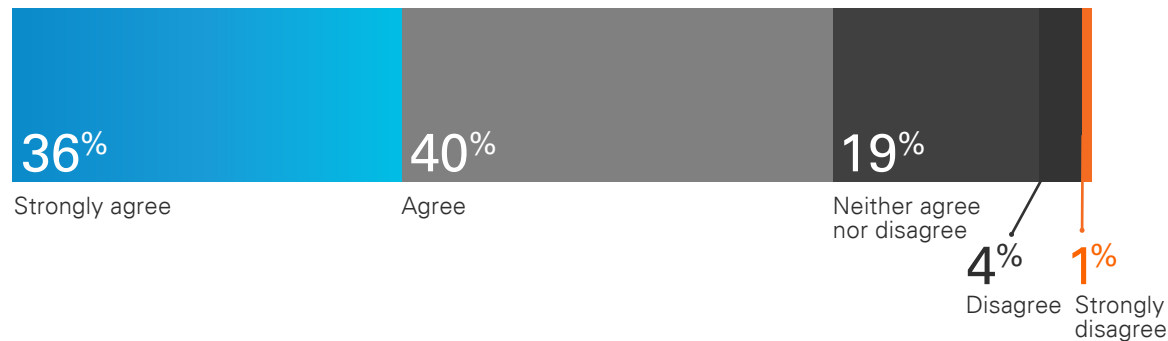


# AI and the digital economy

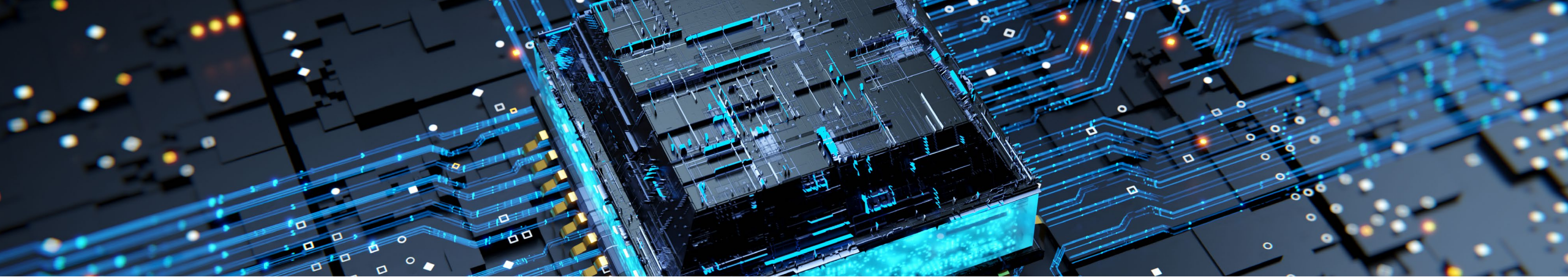
## For consumers, AI creates both opportunities and concerns

The duality of AI as a tool for good and malicious activity is apparent to consumers, who err more on the side of worry than opportunity. Merchants must address these concerns to put consumers' minds at ease.

**AI developments have increased my worry around cyberattacks.**







As AI continues to reshape how people interact with the world, it is also raising consumers' cybersecurity concerns. Only 5% of consumers disagree with the statement, "The recent developments in AI have increased my worry around cyberattacks."

"There's a ton of hype around AI, but the truth is that it's just technology."

— Insurance CISO

While AI can bring numerous benefits to the cybersecurity space, consumers are more

concerned about the malicious activities that can arise from the technology. Many are concerned about voice/video cloning (76%), social engineering messages (72%) and ransomware attacks (54%) utilizing this technology.

CISOs note that the trick is changing the perceptions about the technology and how it can be used for good.

As best summarized by a retail CISO, "we must remember that everybody was also freaked out by the cloud."

The best thing merchants can do to combat concerns over AI is to communicate. Similar to phishing and other malicious activity threats,

businesses must openly communicate with consumers about cybersecurity awareness and educate customers on standard communication processes.

As noted by one CISO, "the quality of the messaging has gone up because it's a lot easier to write an email with AI that sounds more realistic."

Businesses should also be transparent about their use of AI, stressed by 2 in 5 CISOs, and how that will impact the customer experience. By educating consumers about the benefits and threats of AI, merchants can strengthen relationships while also raising consumer awareness around the technology.

## Methodology:

Carat Insights is a regularly produced report focusing on consumer omnichannel preferences. Conducted in August 2024, the most recent report surveyed a national sample of 1,000 U.S. adults employed full time to get their perspectives on cybersecurity and fraud in the current marketplace. Respondents cover all age groups (18 and older), regions and genders. Results from the survey have a margin of error of +/- 3 percentage points.



[Download our Spring 2024 Carat Insights report.](#)



As a global leader in payments and financial technology, Fiserv helps clients achieve best-in-class results through a commitment to excellence and innovation. Carat from Fiserv is the global commerce platform that orchestrates payments and experiences for large enterprise clients.

 [carat.fiserv.com](https://carat.fiserv.com)