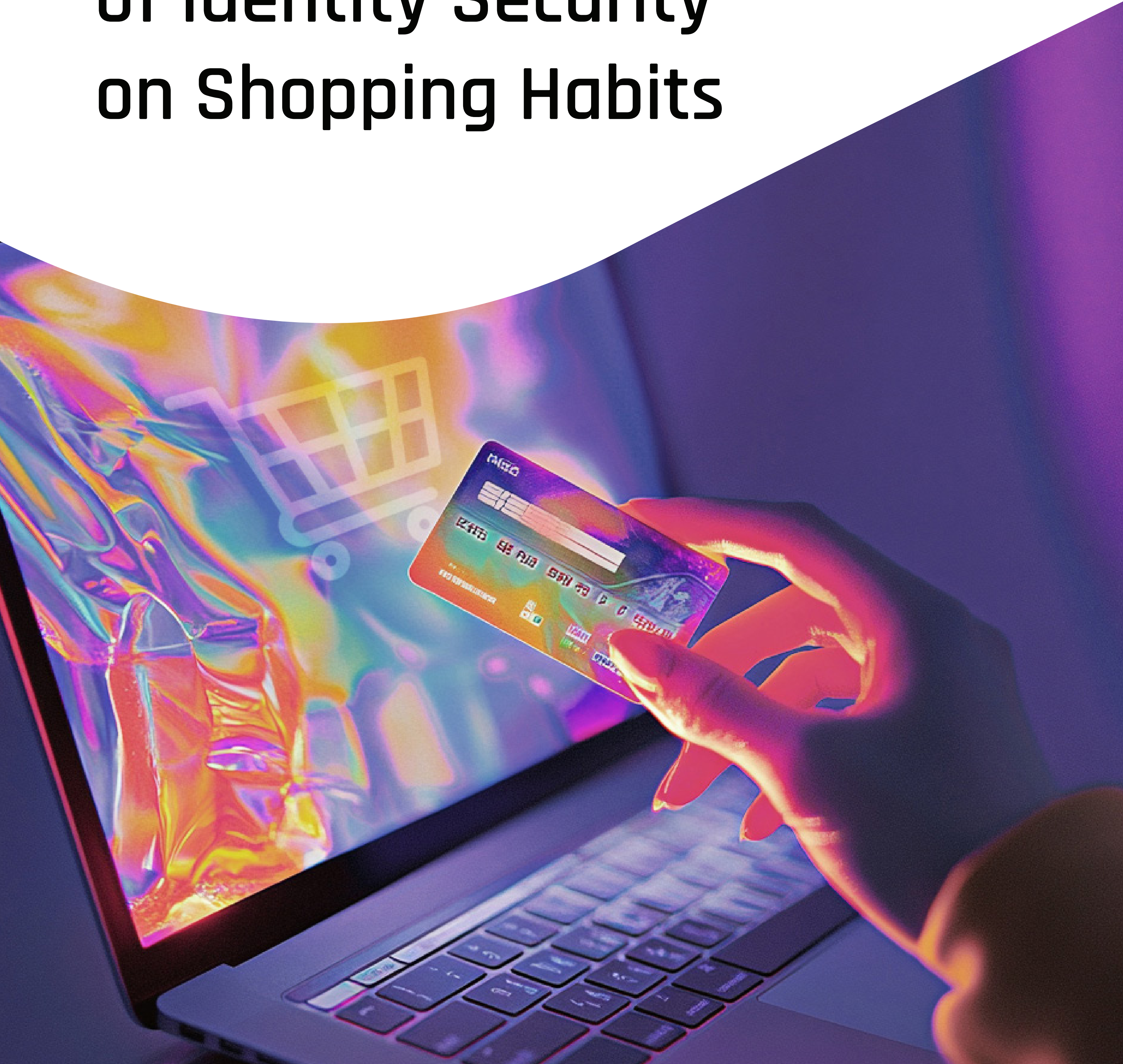
SPOTLIGHT REPORT

HYPR

2024

The Unexpected Impact of Identity Security on Shopping Habits



Introduction

Online retail sales growth has significantly outpaced in-store growth over the past five years,[1] driven by factors including convenience, competitive pricing, social media influence, and personalized shopping experiences. However, recent data suggests this trend may be moderating. According to the U.S. Census Bureau, e-commerce sales in Q2 2024 increased only 6.6% year-over-year — a notable deceleration from historical growth rates.[2]

This slowdown persists even after accounting for the temporary disruptions in shopping patterns during the pandemic shutdown. Analysts attribute the deceleration to multiple factors, ranging from natural market maturation to growing consumer fatigue with the overwhelming array of online purchasing options.[3]

An excess of choice may not be the only thing putting off consumers. Cybersecurity concerns sit top of mind for retailers and their customers alike. A recent TransUnion survey found over half of online shoppers (51%) are concerned about being victimized by online fraud or identity theft.[4]

With its vast volumes of customer and payment information, retail consistently ranks in the top five most attacked sectors. The same technologies that enable retailers to provide quick access and more personalized experiences to consumers, create greater cyber risks. Advisory firm Kroll found a steady increase in breaches in the retail sector, making it the fourth most breached industry last year.[5] Identity, specifically, has become both the key to customer trust and the target of relentless cyberattacks. According to the 2024 Verizon DBIR, credentials were the top data type stolen in retailer breaches, favored even over payment card data. Artificial intelligence has upped the stakes, with retailers collectively experiencing over half a million AI-driven attacks per day between April and September 2024.[6]

To assess the current state of retail cybersecurity, we surveyed a total of 363 individuals, in separate queries of both IT security decision makers at retail organizations, and retail customers.* A distinct trend appears when juxtaposing retail customer concerns and organizations' approaches to identity security. Consumers are growing increasingly worried about the safety of their personal data and privacy, especially as they engage more in online shopping, and they don't trust retailers to protect them.

* IT security decision makers were from retail organizations in the U.S., EMEA and APJ. Retail customers resided in the U.S.

Key Findings

Retail Organizations...

58%

experienced at least one breach related to credential misuse or authentication weaknesses

65%

were the victim of identity fraud in the last 12 months

6.27M

average cost of authentication-related breaches in the last 12 months

Retail Customers...

81%

would stop shopping at a retailer if they had a breach

78%

would be more likely to choose a retailer that offers passkeys

85%

believe there needs to be more regulatory oversight to protect consumers' personal information

Retail Cyberthreat Landscape

Multiple factors make retailers especially vulnerable to cyberattacks. The growth in e-commerce means retailers handle more sensitive data, putting them high on the target list. They often rely on third-party vendors for services like transacting payments and hosting, who themselves are targeted by magecart skimming, cross-site scripting and other threats. Seasonal sales spikes and temporary staffing create more points of vulnerability and opportunities for attack. Moreover, omnichannel operations — physical stores, websites, mobile apps — present unique security challenges, with a weakness in one channel potentially compromising all.

Therefore it's not surprising that an overwhelming majority of retailers surveyed (89%) reported facing cyberattacks in the last 12 months. Phishing, increasingly aided by AI, continues to top the threat list (35%), usually with the aim of stealing credentials to gain access to systems and accounts. In fact, credential and identity-related attacks represented three of the top five attack vectors, including credential stuffing (26%) and identity impersonation (27%). Nearly one-third of retailers (32%) experienced a ransomware attack. Attackers know that retailers cannot afford downtime, particularly during peak seasons, and will likely pay the ransom.

Types of Cyberattacks Faced in the Last 12 Months

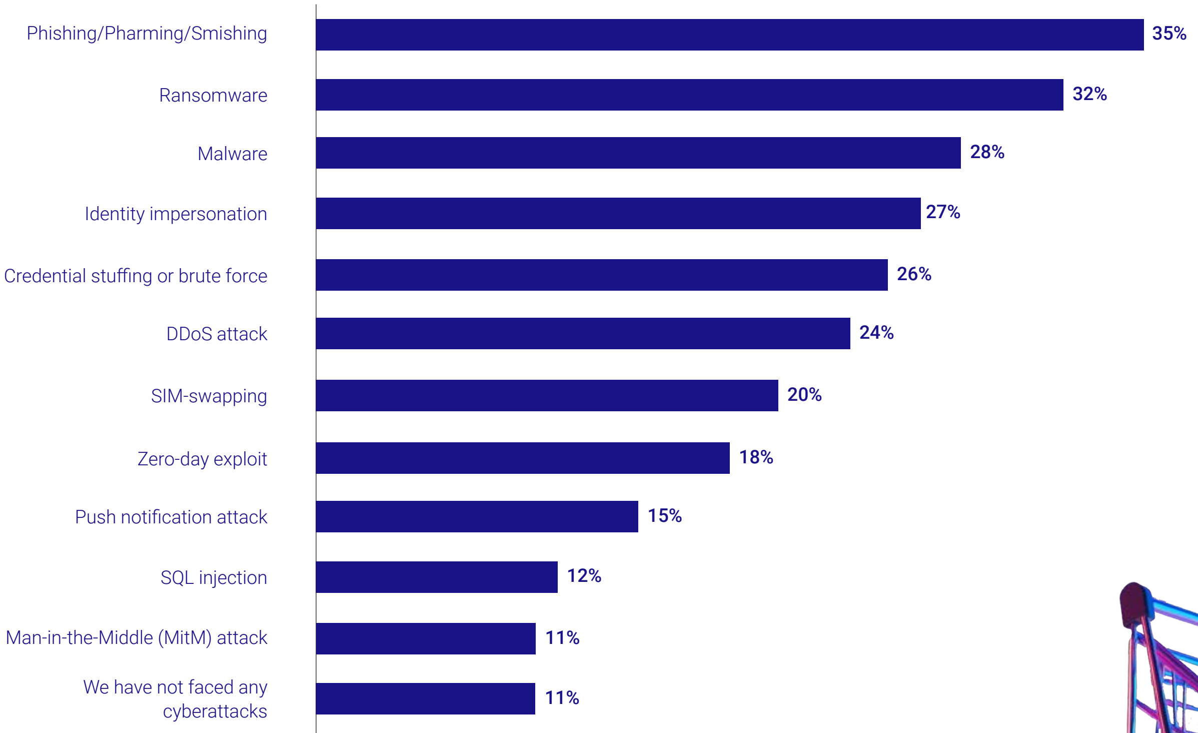


Figure 1: What, if any, types of cyber-attack has your organization faced in the last 12 months?

Identity Process Highly Vulnerable

While not all cyberattacks lead to compromise, 83% of retailers hit by an attack admitted that they experienced a breach. In fact, they experienced multiple breaches — three on average.

When looking at entry points, 78% of the retailers that were breached reported credential misuse or authentication vulnerabilities as the root of at least one breach. This means that nearly six in ten retail organizations (58%) experienced at least one breach related to a weakness in authentication.

The findings clearly indicate that identity practices in the retail industry are leaving systems and data vulnerable. This tallies with other recent industry reports. IBM found the use of valid accounts was the most common initial infection vector in the retail sector, accounting for 43% of breaches.[7]

Breaches Related to Credential Misuse or Authentication Vulnerabilities

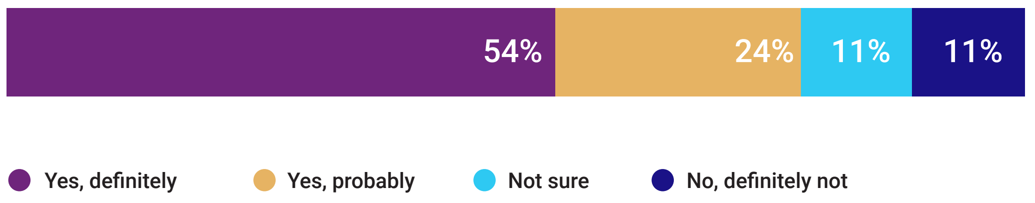


Figure 2: Were any of the cyber-breaches that your organization experienced related to credential misuse or authentication vulnerabilities? Only asked to respondents whose organizations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months

Retailers Feeling the Fallout

With large, loyal customer bases and significant public visibility, retail brands risk significant repercussions from security breaches. A single incident can erode customer trust and have lasting financial impact. Indeed we found that these identity security failures brought far-reaching consequences. More than one-third (35%) of those that were breached lost customers to a competitor and about a quarter suffered reputation damage. Other financial impacts included regulatory fines and lawsuits.

On a positive note, 41% of retailers changed their authentication methods after a breach. Of course the flip side also holds — 59% did nothing to improve their authentication security post breach.

Impacts of Breaches in the Retail Industry

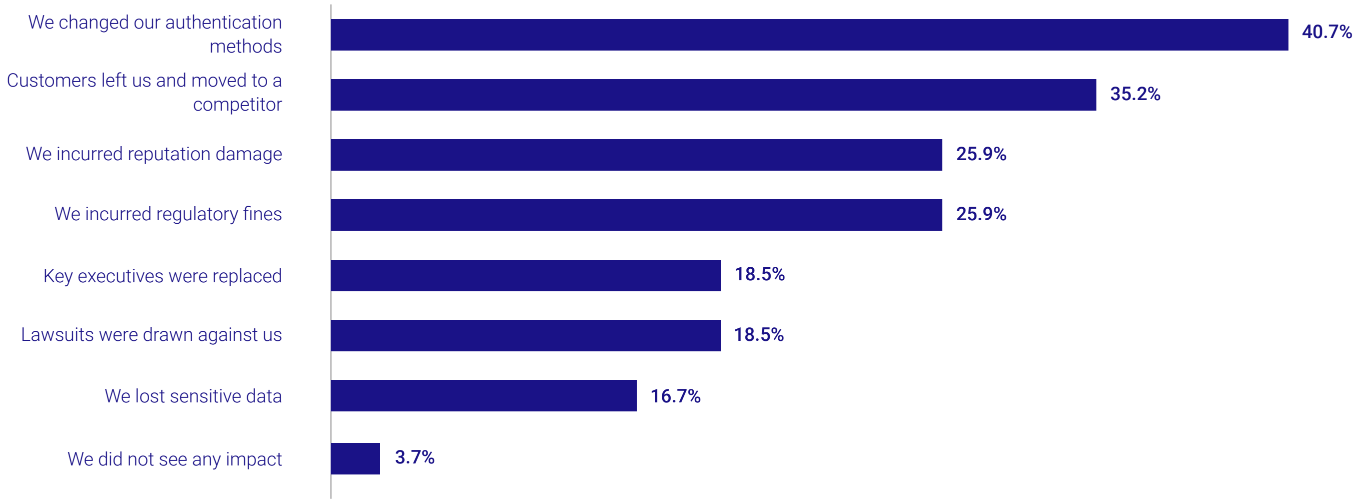


Figure 3: What was the impact of the cyber-breach(es) that your organization experienced in the last 12 months? Only asked to those from organizations that had experienced a cyber-breach in the last 12 months (54), omitting some answer options

Although determining the precise cost of a breach can be tricky, retail businesses state that, on average, breaches caused by insecure authentication caused losses of $6.27 million in the last 12 months.

6.27M

average cost of authentication-related breaches in retail organizations in the last 12 months

Cybersecurity Top of Mind for Customers

Cybersecurity and breaches are a prime concern for retail customers, who expect the brands they shop with to prioritize protecting their data. Shoppers hold retailers responsible for any weaknesses in their security measures. Nearly nine in ten consumers surveyed (88%) stated it is very important that online retailers have strong security measures in place to protect their personal information; less than 2% said it's only slightly important or had no opinion.

What Threats Are Retail Customers Most Worried About?

Despite the continued growth in e-commerce, nearly all consumers (97%) feel uneasy about cyberthreats when shopping online. The possibility of payment card theft (88%) and identity theft (74%) head their list of concerns. They are also well aware of specific threats lurking, with seven in ten expressing worry about cybercriminals capturing their login information, and half that they will be tricked by fake shopping sites and apps.

Top Online Shopping Threat Concerns

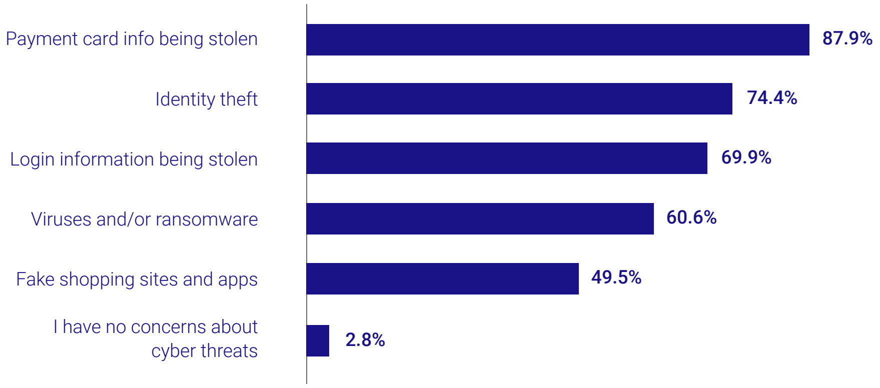
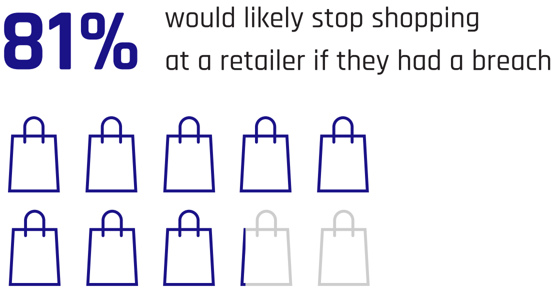


Figure 4: What cyber threats are you most worried about shopping online?

Brand Loyalty On the Line

More than eight in ten consumers (81%) state that they would cease shopping at a retailer if they had a breach. This figure held true across different age groups. That contrasts sharply with a similar survey of finance customers, which found customers over 45 were four times more likely than those under 35 to remain with their financial institution after a security breach. The lesson? Brand loyalty must be continually earned, even for long-time retail customers.

Likelihood of Customers Abandoning a Brand After Data Breach



While retailers should rightly worry about this figure, we saw in the previous section that only 35% of breached retail organizations reported customer loss as a result. This could indicate that old shopping habits die hard or, more likely, that customers remain unaware when breaches occur.

Passkeys on Shopper's Wish List

Today's shoppers are highly aware of cybersecurity advancements and expect retailers to stay ahead in protecting their data. Although passkeys became available only two years ago, the majority of retail customers (95.5%) have at least heard of them and almost 20% claim to have a working knowledge of the technology. Education is still needed, however, as about a third do not understand the difference between passkeys and passwords or have not heard of them at all.

Customer Passkey Knowedge Levels

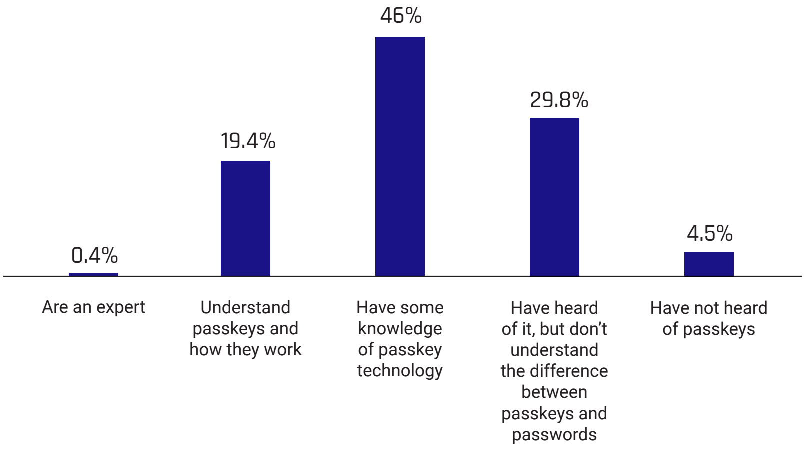


Figure 5: How familiar are you with passkey technology?

In fact, passkeys provide a distinct competitive advantage to retailers that offer them. Nearly eight in ten consumers (78%) prefer to shop with a brand that offers passkeys. With shopper loyalty weakening across all demographic groups, according to a recent report by McKinsey & Co.,[9] every retailer with an online operation should be planning to offer passkeys, if they don't already.

78%

of customers would be more likely to choose a retailer that offers passkeys

Security Measures Used by Consumers

For the most part, consumers practice what they preach security-wise. When shopping online, nearly half (49%) use passkeys when offered, more than eight in ten (83%) use multi-factor authentication and 84% make sure to use strong passwords. However, this means that 16% persist in using weak passwords. Moreover, 46% do not use any form of antivirus protection and 49% will shop using public WiFi. Interestingly, those consumers aged 45 and up tend to take cybersecurity most seriously, choosing MFA, using antivirus, and avoiding public WiFi at rates more than ten percentage points higher than their younger counterparts.

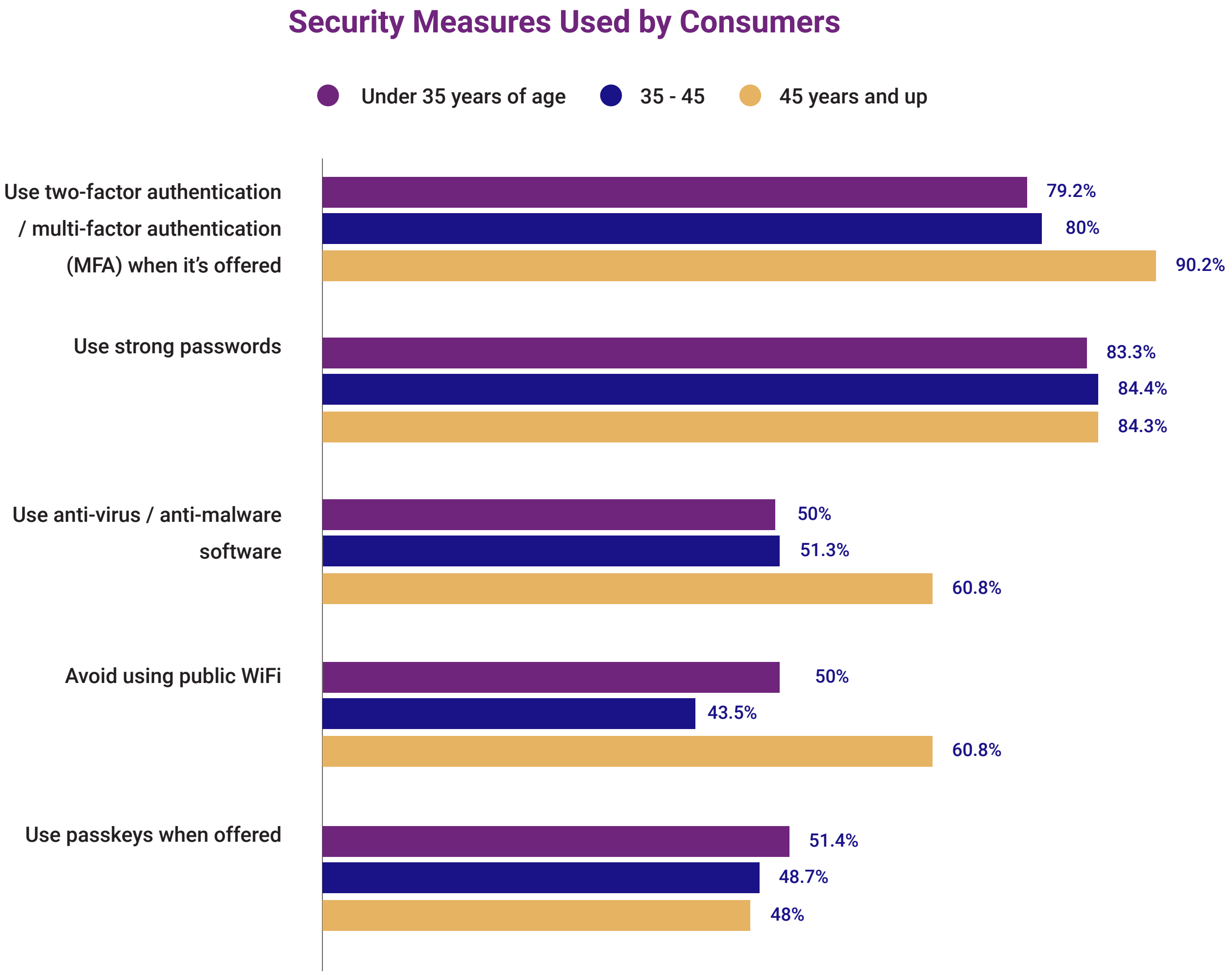


Figure 6:What actions do you typically take to protect your personal information when shopping online?

Passkeys Wanted But Retailers Lagging

Although shoppers are pushing for passkeys, rollout by retailers remains slow. Less than a quarter (23%) plan to offer passwordless / passkey authentication to their customers within the next three years. Cost, not implementation complexity, appears to be the main reason for the delay. More than four in ten retailers (42%) identify implementation costs as a top barrier to adoption while only 26% name implementation challenges. Interestingly, 11% say there are no challenges at all – more than double the average across all industries.

Over the next three years, most retailers will stick to a mix of less secure customer authentication methods. Nearly half (46%) will let customers log in using only a username and password, 53% will offer traditional MFA approaches, and 45% will continue offering social identity credential logins.

Authentication Technologies for Customers In Use and Planned

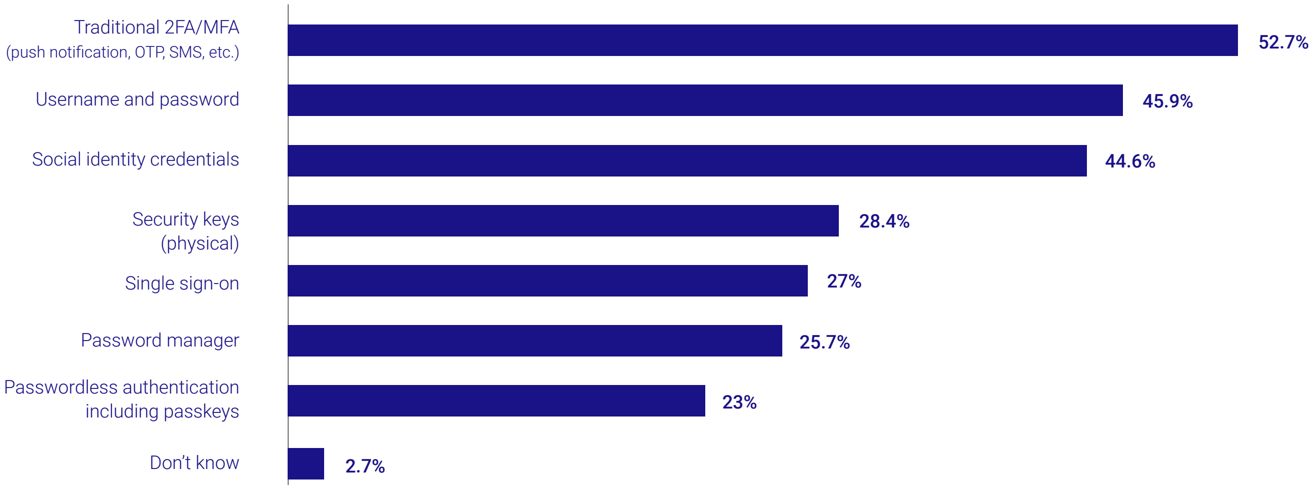


Figure 7: Which of the following authentication methods does your organization plan to adopt, or use/continue to use in the next 1-3 years for customers? omitting some answer options

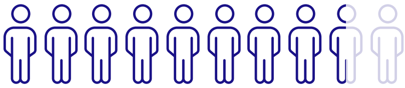
Customers Don’t Trust Retailers to Protect Their Data

When it comes to data protection, retail customers don’t necessarily trust the businesses they shop with to do the right thing. Retailers already contend with a tangle of data security requirements. These include, depending on the types of data they process and where they and their customers are based, PCI DSS, PSD2 SCA, HIPAA, GDPR and CCPCA.

Despite regulations already on the books, the vast majority of retail customers (85%) believe that the government needs to step in to ensure their personal information is safe from data breaches. Surprisingly, this figure stayed fairly consistent across all age brackets.

We should note that this survey consisted of U.S. retail customers only and did not question about state residence. Additional data would be needed to determine if those consumers already protected by laws such as GDPR and CCPA feel the same need for additional regulatory oversight.

Desire for Regulatory Oversight



85% of consumers believe that government regulations should play a greater role in protecting consumers’ personal information from data breaches in the retail space

Conclusion

As the retail industry continues to evolve and modernize, businesses grapple with a constantly shifting landscape of security threats. Generative AI has become both a powerful tool and a potential risk for retailers — streamlining operations and enhancing customer experiences while also introducing new vulnerabilities. In this interconnected world, identity has become the new security perimeter, and as these findings show, it's the greatest point of risk.

Retail customers, increasingly aware of these risks, are raising the bar for security expectations. They have a strong interest in modern protections like passkeys and expect the retailers they trust to lead the way in adopting these innovations. Customer loyalty depends on how well retailers rise to these challenges.

Fortunately, these technologies are already mature and offer benefits beyond security. They bring faster access, reduced support costs and a smoother experience for customers. The sooner this technology reaches consumers, the stronger and more resilient the retail sector will become.

How HYPR Can Help

HYPR is a pioneer in FIDO passkey-based authentication, and is deployed and battle-tested in some of the largest organizations in the world. The HYPR Identity Assurance platform combines frictionless passwordless authentication, proactive risk controls and integrated identity verification to stop modern identity attacks while reducing customer frustration. Our mobile and web SDKs are geared towards flexible, easy deployment so that you can immediately remove passwords from your customer experience. Learn how HYPR can help secure your customers and business at hypr.com/demo.

Appendix: Approach and methodology

The insights in this report were derived from two separate surveys:

1) HYPR commissioned independent technology market research specialist Vanson Bourne to survey 750 IT security professionals in February and March of 2024 for its 2024 State of Passwordless Identity Assurance report, published May 2024. The survey included 74 respondents in the retail sector. This report uses the retail survey data to uncover findings specific to that sector. Interviews were conducted online using a rigorous multi-level screening process.

2) The customer research survey was conducted in June 2024 through Userlytics, a research panel company. The sample consisted of 289 US-based consumers. Respondents were invited to take the survey and informed that it was research on attitudes about online shopping security. Participants were incentivized to participate via the platform's established compensation program.

Sources

[1] https://capitaloneshopping.com/research/online-vs-in-store-shopping-statistics/
[2] https://www.pymnts.com/news/retail/2024/ecommerce-now-15-2-percent-of-retail-sales-as-growth-slows/
[3] https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Empowered-Consumer.pdf
[4] https://www.transunion.com/content/dam/transunion/us/business/collateral/report/2023-Holiday-Shopping-Report.pdf
[5] https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2024
[6] https://thehackernews.com/2024/11/cyber-threats-that-could-impact-retail.html
[7] https://www.ibm.com/reports/threat-intelligence
[8] https://www.hypr.com/resources/report-customer-identity-security-in-finance-2024
[9] https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/state-of-consumer#/

See how HYPR helps secure your retail organization and customers

Visit: hypr.com/demo

HYPR

THE IDENTITY ASSURANCE COMPANY

www.hypr.com | hypr.com/contact

About HYPR

HYPR, the leader in passwordless identity assurance, delivers the industry's most comprehensive end-to-end identity security for your workforce and customers. By unifying phishing-resistant passwordless authentication, adaptive risk mitigation, and automated identity verification, HYPR ensures secure and seamless user experiences for everyone. Trusted by organizations worldwide, including two of the four largest US banks, leading manufacturers, and critical infrastructure companies, HYPR secures some of the most complex and demanding environments globally.