KnowBe4

Global Retail Trends: Stolen Credentials Emerging As A Top Threat

Over 62% of all purchases are made with a credit or debit card.[1] When a customer uses a card to make a retail purchase, whether online or in store, they are entrusting that retailer with their credit card and other Personally Identifiable Information (PII), including their name, address, and phone number. If they access their account on the web or through the store's Point of Sale (POS) system, the retailer also has their past purchasing information and tracking data including any changes of addresses, and other addresses they have sent packages to.

Consequently, it should come as no surprise that the retail sector has become a nearly irresistible trove for a growing number of cybercriminals. Unfortunately, new AI tools have not only enhanced the abilities of experienced cybercriminals, but also given state-of-the-art intrusion methods to relatively unskilled or novice attackers.

If typing the card verification value (CVV) code of a debit card onto a website to make a purchase or handing over a credit card in a store is contingent on the customer's trust in the transaction, no retailer can afford to be less than vigilant and proactive in protecting what their customers have placed on their servers.

Rising Frequency and Cost of Cyberattacks in Retail

Across the board, the most reputable studies of trends in cyberattacks are finding an alarming increase in the frequency of attacks against the global retail sector.

The 2024 Verizon Data Breach Investigations Report (DBIR),[2] which collected and analyzed global cyberattacks from November 22 to October 31, 2023, recorded and analyzed 725 incidents in the retail sector. Of these, 369 were confirmed as having resulted in data disclosure. The 2023 total for retail was 56% higher than 2022's figure of 404 incidents, 191 of which resulted in disclosure.

IBM X-force, the company's team of crack cybersecurity researchers, analysts, responders, and even hackers, found a similar trend in its 2024 report.[3] The retail and wholesale sector accounted for 10.7% of all attacks globally in 2023, putting it in the top five sectors attacked. The frequency of attacks against the sector increased by 25% over 2022.

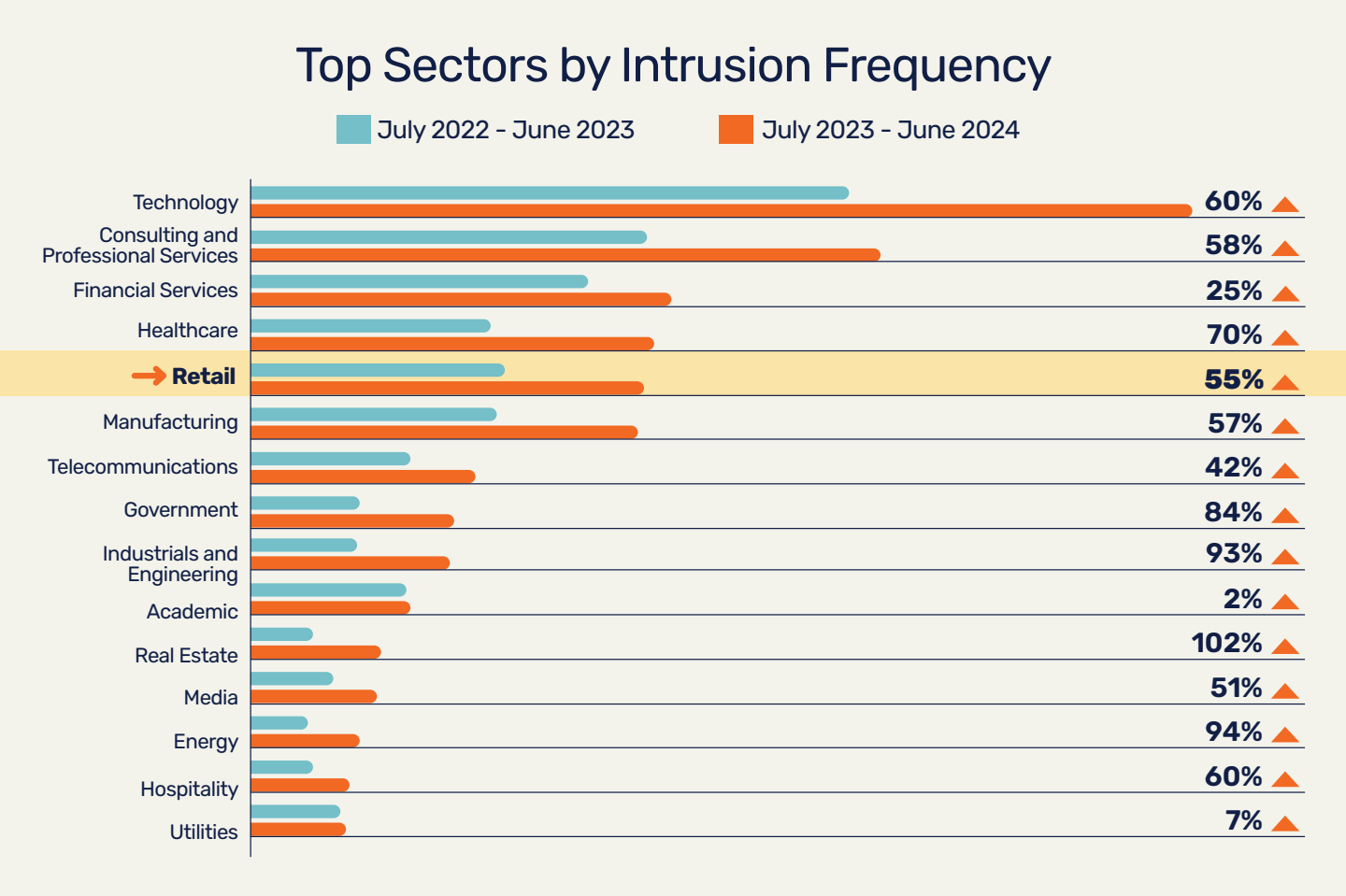
Retail is in the top five industries targeted by cybercriminals.

CrowdStrike's 2024 Threat Hunting Report[4] measures cyberattacks taking place between July 2023 and June 2024. Here, again, the retail sector came in the top five of all sectors attacked, alongside technology, consulting and professional services, financial services, and healthcare. With the first two quarters of 2024 data factored in, the frequency of attacks against the retail sector is even higher than the others, showing a 55% increase year over year.

While becoming more frequent, the attacks are also getting more expensive. The IBM Cost of a Data Breach Report[5] is based on an in-depth analysis of real-world data breaches experienced by 604 organizations globally between March 2023 and February 2024. The report places the average cost of a data breach in the retail sector in 2024 at $3.48 million, an 18% jump from $2.96 million in the 2023 report. The cost of a breach in the Consumer Packaged Goods (CPG) was even higher, at $3.91 million.

Contributing to the rising costs, the "hidden" costs — including lost business from system downtime, the loss of customers and reputational damage, and post-breach expenses, such as setting up call centers, providing credit monitoring services for impacted customers, and paying regulatory fines — increased by nearly 11% from the previous year.

Some of these costs may not show themselves until years after the breach. In early November 2014, when a third-party vendor of Home Depot was hacked, the hackers used a vendor's stolen login credentials to gain entry to the Home Depot system, then deployed malware designed to infect the retail giant's POS system and exfiltrate customer payment information. Between April and September 2014, the hackers accumulated data on 53 million Home



Depot customers. Home Depot paid $17.5 million to settle claims across the country. But that was just the start. The company ended up paying more than $215 million for the breach, most of it related to litigation by customers, payment card issuers, and financial institutions.

Perhaps the most expensive cyberattack in the retail sector to date was in 2013 and began with a successful spear phishing attack on a third-party vendor, which allowed the hacker to use stolen credentials to compromise Target's network. Once in, they installed malware to steal customer data over a period of two months, ending up with both payment card and contact information of 41 million customers, and contact information only for a further 70 million customers. Target paid fines totaling $18.5 million, ultimately paying $290 million for the breach, including costs of remediation, consulting fees, and other payments.

Which Countries are Most at Risk?

IBM notes that North America's retail sector experienced the highest percentage of attacks(56%), while Latin America saw the second most at 32%, and Europe experienced 11% of attacks.[6]

When threat intelligence provider Cyberint (a Check Point company) analyzed incident data on ransomware,[7] they found that while the U.S. retail sector only accounted for 28% of global market share, it experienced 45% of ransomware attacks. This was a 9% increase in the U.S. "share" of the attack horizon over the same period in 2023.

Looking across all sectors in the U.S., the retail sector accounted for 14% of the total 1,634 ransomware incidents across all industries. This was a 40% increase in retail's "share" of ransomware attacks over the same period in 2023; it moved retail into second place among the most targeted sectors.

A Global Snapshot of Cyberattacks in Retail

JD Sports, U.K. In 2023, fashion retailer JD Sports was hit with a major cyberattack in which a server containing online order information for customers was hacked. In its official announcement, the company said the cybercriminals responsible had stolen information that included: "…the name, billing address, delivery address, email address, phone number, order details and the final four digits of payment cards of approximately 10 million unique customers." The breach impacted many of the company's group brands, including JD, Millets, Blacks, Scotts, and MilletSport. The attackers then used the data stolen to launch social engineering attacks against exposed individuals.

Supermarket chain, Japan. In February 2024, a ransomware attack crippled the ordering system of a Japanese regional supermarket chain. Recovery was slow, taking over two and a half months to fully restore operations. Details, including the name of the chain, were not released to the press.

Fourlis Group, Greece. Retail group Fourlis suffered a ransomware attack in November 2024 that affected the group's operations in Greece, Cyprus, Bulgaria, and Romania. The attack brought down IKEA's online store in several countries where Fourlis holds the franchise.

Pepco Group, Hungary. On February 27, 2024, Hungarian discount retailer Pepco Group announced that it had been the target of a phishing attack that resulted in the loss of €15 million (USD $16.3 million). Further details were not offered by the company, other than that the incident does not appear to have involved any customer, supplier, or staff information/data, raising speculation that the attack may have involved Business Email Compromise (BEC).

London Drugs, Canada. On April 28, 2024, a ransomware attack forced Canadian pharmacy chain London Drugs to close 80 retail stores across Western Canada. It appears that no customer databases or health data were compromised, but employee personal information was stolen. A month later, while stores had reopened, the company's website was still down. LockBit claimed responsibility for the attack.

Kadowaka Corporation, Japan. In June 2024, the Japanese publishing group's data center was hit by a ransomware attack that caused a systemwide crash, leading to delays in publication deliveries and bringing the organization's video streaming service to a halt. The impact to the company, including loss of customer confidence, was compounded by the fact that Kadowaka did not disclose that customer data had been breached for nearly three weeks.

Co-op Group, Sweden. A ransomware incident in June 2024 disrupted the operations of one of the largest retail and grocery providers in Sweden, with approximately 800 stores across the country. The attack paralyzed the company's POS systems, making it impossible to process payments. Over 500 of the retailer's stores were forced to close temporarily, resulting in substantial financial loss and inconvenience to customers, eroding trust and satisfaction. The attack caused logistical nightmares, as supply chains and inventory management systems were also affected. The Cactus ransomware operation claimed responsibility.

Hot Topic, U.S. Pop culture retailer Hot Topic and its subsidiaries Torrid and Box Lunch were breached in November 2024, impacting 54 million email addresses and weakly encrypted credit card information for 25 million users. The breach likely began with a malware infection on the device of an employee of Robling, a retail analytics company used by Hot Topic. If so, the attacker may have planted an infostealer on the device, which allowed the attacker to gather approximately 240 credentials.

Blue Yonder, global. On November 21, 2024, Arizona-based supply chain software company Blue Yonder was hit with a ransomware attack that disrupted the company's operations, as well as those of several major firms that use its services, including Starbucks, two of the UK's biggest grocery store chains - Morrisons and Sainsbury's - and British bookseller Waterstones. Blue Yonder provides systems for fulfillment, delivery and returns for more than 3,000 major companies across 76 countries. An emerging ransomware group named Termite Ransomware claimed credit for the attack and claimed to have stolen 680GB of Blue Yonder data.

How Cybercriminals Infiltrate Retail Organizations

Social engineering – manipulating someone to do something against their own best interests – remains central to most intrusion methods used by cybercriminals.

Recent reports highlight the prevalence of social engineering in cyber threats across sectors. The Avast Q1/2024 Threat Report[8] reveals that social engineering tactics were involved in an overwhelming majority of cyber threats, accounting for 90% of mobile and 87% of desktop threats. This trend is mirrored by an additional report that analyzed 23.5 billion cyberattacks in 2022, which found that 80-95% of all attacks were initiated through phishing.

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC), a trusted community for sharing cybersecurity information and intelligence in the sector, also stated in their 2024 report that phishing and credential harvesting remain the primary intrusion vectors in attacks, noting that: "Members report a steady prevalence in phishing attempts with lure themes involving popular product promotions targeting consumers for PII harvesting."[9]

The Weak Points

There are several factors that create relatively easy entry points for attackers and make the retail sector particularly vulnerable to attack.

Seasonal events and changes

With events like Christmas, Black Friday and back-to-school sales during seasonal transitions, there is a significant increase in traffic and digital payment transactions. Particularly as the December holiday season approaches, the workforce often becomes overextended, and stores struggle with employee shortages and turnover. The influx of seasonable employees means a wave of personnel with little-to-no cybersecurity awareness or training and limited experience with company security policies, making them a tempting target for cybercriminals. IT teams may also grow stretched over the season as they deal with new waves of cyber alerts and insufficient time to stay on top of the growing sophistication of methods of attack, creating a "perfect storm" of risk.

Third-party dependencies

Retailers frequently rely on a network of outside vendors for payment processing, logistics, shipping, and other services. As noted in the examples above, each of these supply chains present a potential entry point for threat actors; a breach at any third-party vendor, particularly when credentials are stolen, can cascade and compromise the retailer's system.

One of the most dramatic examples of this vulnerability occurred in June 2024, when cloud storage firm Snowflake, which stores huge databases for its customers, revealed that hackers had been attempting to access its customers' accounts using stolen login details. On June 5, 2024, *TechCrunch*[10] reported that hundreds of Snowflake customer passwords had been found online from an information stealer, including U.S. bank Santander, Ticketmaster, at least two pharmaceutical giants, a food delivery service, a public-run freshwater supplier, and others. Hacker groups surfaced with a devastating 560 million Ticketmaster records for sale, confirmed to have come from the Snowflake breach, along with another 30 million records from Santander Bank. Others appeared with 380 million records from automotive giant Advance Auto Parts and 190 million records from financial services company Lending Tree; all stemming from the Snowflake database breach.

On June 17 of the same year, Wired reported[11] that the hackers had originally obtained access to the Ticketmaster's Snowflake cloud account—and others—by first breaching the account of a contractor, EPAM, that provided software engineering services for the companies. EPAM, originally founded in Belarus, now operates in the U.S., across Europe, and in Latin America. The hacker who spoke with Wired about the initial breach reported that one of the EPAM computers was infected with infostealer malware through a spear phishing attack. Mandiant, one of the companies engaged by Snowflake to investigate the breaches, confirmed in a blog post[12] that in some cases, the hackers first obtained access through third-party contractors. The hackers were able to use those credentials to access the Snowflake accounts, according to Wired, because the Snowflake accounts did not require multifactor authentication (MFA) to access them but are available on a per-user basis.

While the Snowflake breach was "snowballing," AT&T telecom giant had learned of a breach involving Snowflake that they had not yet disclosed. On April 19, 2024, the company learned that hackers had accessed files containing AT&T call detail records (CDRs) of nearly all theirs cellular customers — more than 100 million users. AT&T contacted the FBI to report the incident, and all parties agreed to delay a public announcement to avoid undermining investigation into the breach, and because of potential risks to national security and/or public safety. The breach was not announced until AT&T issued a press release on July 12. On July 14, 2024, Wired[13] reported that AT&T had paid the hacker $370,000 in bitcoin to delete the stolen records.

It all started with one spear phishing attack on one computer of one supplier halfway around the world.

Multichannel operations
The modern retail environment creates a complex and broad attack surface, combining brick and mortar stores with digital POS systems, e-commerce websites, mobile applications, payment installment programs, gift card processing, and other digital touchpoints. A vulnerability in one element can compromise the entire network.

Franchise vulnerabilities
While operating semi-autonomously, franchises can create inconsistencies in security policy. Single franchises may lack resources or knowledge in effective implementation of security practices. A compromised franchisee can negatively impact the franchisor's reputation and brand.[14]

What Hackers are After

We already know that cybercriminals in the retail sector are after the money; it is no surprise that the Verizon report found that 99% of the threat actors in the sector were motivated by financial gain (the remaining 1% were motivated by espionage). But a surprising shift occurred in 2023.

In past years, attackers have primarily targeted payment card data, which could then be sold or quickly used for fraudulent purposes. In 2023, credential harvesting, which involves capturing sensitive information like login credentials, browser session cookies, payment card details, autofill data, and more, accounted for 38% of all compromised data. This marks an increase, while payment card details dropped from 37% to 25%.[15]

This trend may be due to increased controls on card usage by banks. In contrast, stolen credentials allow attackers to bypass standard authentication processes and gain immediate access to personal accounts. Access to session cookies, along with login details, enables attackers to bypass passwords and two-factor authentication (2FA).

Traditional data sources within organizations are also vulnerable to attack, including databases of customer information, intellectual property valuable to competitors, and other proprietary information.

Getting Ahead of the Breach

The ReliaQuest Annual Threat Report: 2024[16] provides further evidence of phishing's dominance in cyber threats. The report shows that in 2023, phishing links or attachments were involved in 71% of all initial access phases of cyberattacks. Notably, spearphishing was the preferred attack vector among cybercriminals. This further emphasizes the ongoing significance of phishing as a primary entry point for malicious actors.

Fortunately, that risk can be measured, monitored, and reliably managed.

Each year, KnowBe4 conducts initial phishing simulation tests within organizations that have not conducted any security awareness training from

the KnowBe4 platform. The tests are conducted without prior alerts, targeting individuals performing their routine work tasks without any specialized training. These tests result in a baseline Phish-prone Percentage™, or PPP, that shows the percentage of employees who are prone to click on a phishing link. This is further broken down and applied to specific industries and geographic regions.

Spanning all industries and organizational sizes, the 2024 KnowBe4 Phishing by Industry Benchmarking Report[17] found that the average PPP stood at 34.3%. In other words, as a baseline, more than one in three employees are inclined to interact with malicious encounters or click on a link in a malicious email.

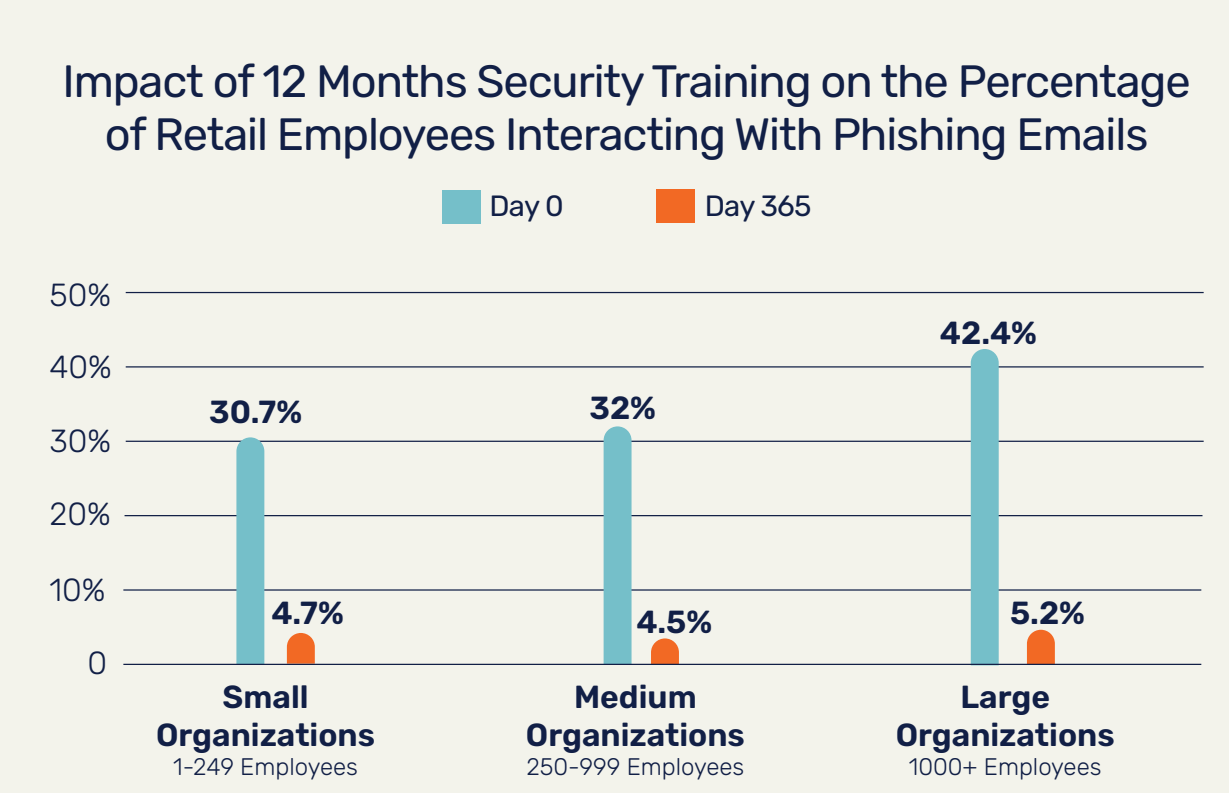
In the retail and wholesale sector, the baseline PPP for small companies with 1-249 employees was 30.7%. For companies with 250-999 employees, the PPP is 32%. Large companies with more than 1,000 employees fared the worst, with 42.4% of employees inclined to click on a phishing email.

After 90 days using an integrated approach of educational content along with simulated phishing tests, outcomes were significantly improved in the retail and wholesale category, with PPPs reduced to 20.6% for small companies, 21.1% for medium-sized companies, and a dramatic drop from 42.4% to 18.3% for companies with over 1,000 employees.

After one year or more of sustained training and simulated phishing evaluations, the year-over-year findings are consistently impressive, reinforcing the impact of a steady, well-developed security awareness training program. In retail and wholesale industries, the average PPP for small companies with sustained training dropped to 4.7%. For medium-sized companies, it dropped to just 4.5% and to 5.2% for large ones.

Reducing Human Risk in Retail

The retail sector faces an escalating threat from cybercriminals, with stolen credentials emerging as the top concern. The increasing sophistication of attacks, coupled with the sector's inherent vulnerabilities, necessitates a proactive approach to cybersecurity. Implementing robust security awareness training programs has shown significant promise in reducing human risk factors, which account for the majority of data breaches. As the threat landscape evolves, retailers must prioritize cybersecurity measures, including employee education, to protect their customers' data and maintain trust in an increasingly digital marketplace.



Endnotes

1 "2024 Findings from the Diary of Consumer Payment Choice," Federal Reserve Bank Services, https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2024-diary-of-consumer-payment-choice.pdf
2 "2024 Data Breach nvestigations Report," Verizon, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
3 "IBM X-Force Threat Intelligence Index 2024," IBM, https://www.ibm.com/reports/threat-intelligence
4 "CrowdStrike 2024 Threat Hunting Report," CrowdStrike, https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
5 "Cost of a Data Breach Report 2024," IBM, https://www.ibm.com/reports/data-breach
6 *"IBM X-Force Threat Intelligence Index 2024,"* IBM, https://www.ibm.com/reports/threat-intelligence
7 "Retail Threat Landscape Report Q1-Q3 2024 Summary, https://e.cyberint.com/hubfs/Retail_Threat_Landscape_Report_Q4_2024.pdf
8 Q1/2024 Threat Report, Avast, https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report
9 "2023 Holiday Season Cyber Threat Trends," PH-ISAC, https://rhisac.org/wp-content/uploads/Holiday-Trends-Report-2023_Clear.pdf
10 Whittaker, Zack, *"Hundreds of Snowflake customer passwords found online are linked to info-stealing malware,"* TechCrunch, June 5, 2024, https://techcrunch.com/2024/06/05/snowflake-customer-passwords-found-online-infostealing-malware/
11 Zetter, Kim, *"Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake,"* Wired, June 17, 2024, https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/
12 *"UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion,"* Threat Intelligence, Mandiant, June 17, 2024, https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
13 Zetter, Kim *"AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records,"* Wired, July 14, 2024, https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/
14 *"2024 Trustwave Retail Risk Radar,"* Trustwave, https://www.trustwave.com/en-us/resources/library/documents/trustwave-spiderlabs-research-defending-the-retail-sector-in-2024/
15 *"2024 Data Breach Investigation Report,"* Verizon, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
16 "ReliaQuest's Annual Cyber Threat Report: 2024" https://www.reliaquest.com/resources/research-reports/annual-threat-report-2024/
17 *"2024 Phishing By Industry Benchmarking Report,"* KnowBe4, https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com