BUYERS GUIDE

SpyCloud

CONSUMER RISK PROTECTION

GUIDE TO

Preserving Account Integrity & Reducing Risk

WHAT'S INSIDE

BUYERS GUIDE

INTRODUCTION

As criminals exploit stolen data for malicious activities – from fraudulent transactions to identity theft – **the security of customers' accounts and their personal information is a top concern for security teams**. The surge in stolen personal and authentication data traded on the criminal underground, coupled with sophisticated criminal tactics, presents security practitioners with an ever-growing challenge: how to distinguish between legitimate customers and criminals using stolen information.

How we protect consumers and our businesses has to evolve just as rapidly as the tactics bad actors use to infiltrate and steal data. It's a collaborative effort across multiple teams – Application Security, Information Security, Fraud, Identity, Governance, Risk and Compliance, and Security Operations – to build programs that reduce risk, while also maximizing business productivity and maintaining low friction for customers.

SECURE CONSUMER DATA + **UPHOLD BRAND REPUTATION** + **PREVENT FRAUDULENT TRANSACTIONS**

This guide explores the challenges of today's landscape and provides insights into how SpyCloud's **Consumer Risk Protection** solution eliminates the guessing games and serves as a critical ally in addressing evolving threats.

IN THIS GUIDE

You'll learn more about navigating the complexities of modern account takeover methods and how to strengthen account security by using insights into a consumer's exposures in the criminal underground. We'll cover:

- Challenges teams face in determining if a user is a legitimate customer or a criminal that adds burden to your operations and impacts your brand's market perception
- How SpyCloud helps your team quickly and accurately mitigate risk
- Operational efficiencies and business outcomes you can expect from using SpyCloud

Let's dive into how you can fuel a resilient security posture with SpyCloud.

TODAY'S RISK LANDSCAPE

Why customer account protection is hard, and getting harder –

While the goal to keep customer accounts secured is clear, the challenges stolen data brings to the table are worth exploring. Understanding the root causes of the **"customer or criminal?"** question is essential in building and maintaining strong security frameworks.

1 Human Behavior Drives Account Risk

Account security is paramount today more than ever, with customers relying on brands to safeguard their sensitive information. However, human behavior plays a significant role in driving account risk, as individuals often unwittingly expose themselves to cyber threats through their actions. This necessitates proactive measures to address vulnerabilities and protect against various forms of attacks.

CUSTOMER EXPECTATIONS VS. BEHAVIOR

- Customers expect brands to keep their accounts safe, but their actions contribute to online risk.
- Individuals often use weak passwords and reuse them across multiple sites for convenience, inadvertently increasing vulnerability.

CREDENTIAL STUFFING ATTACKS

- Cybercriminals leverage compromised credentials in automated attacks, gaining unauthorized access to accounts on various platforms.
- Security teams must implement checks during account creation to identify previously exposed credentials and mitigate the risk of automated attacks.

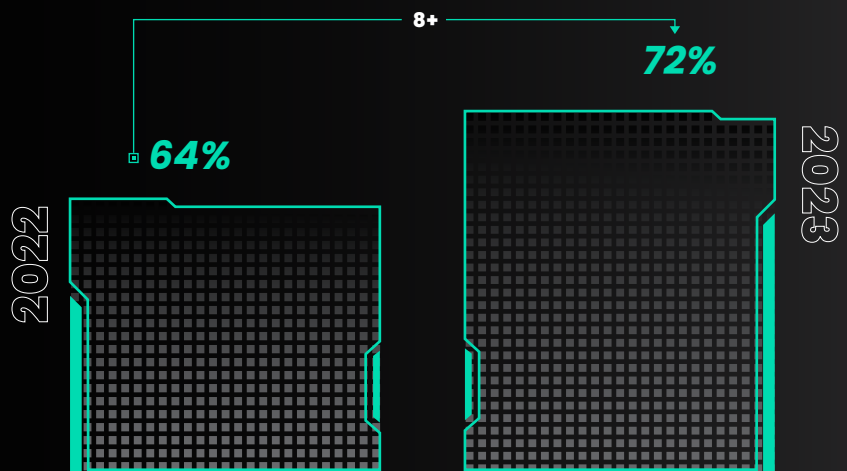
RISE OF SOPHISTICATED MALWARE CAMPAIGNS

- Malicious actors are enhancing malware campaigns, leading to an increase in phishing schemes and malicious downloads.
- These attacks compromise devices and facilitate the theft of sensitive information, including authentication data.

PREVENTION STRATEGIES

- Security teams need to detect malware-infected users and stolen cookies to prevent emerging forms of account takeover and safeguard user accounts.

SpyCloud's annual analysis of recaptured data from the darknet shows an **all-time 72% password reuse rate** for users exposed in two or more breaches, a **8-point increase** from the previous year's all-time reuse rate.



2 Too Much Data, Not Enough Context

In the ever-evolving landscape of cybersecurity, the challenge lies not only in the sheer volume of data but also in its contextual relevance. Without sufficient insight into the circulation of sensitive data on the darknet, including stolen authentication data like passwords and session cookies, organizations remain vulnerable to account breaches and fraudulent activities.

VISIBILITY AND CONTEXTUAL UNDERSTANDING

- Lack of visibility into credential, identity, and financial data on the darknet allows attackers to exploit vulnerabilities without triggering existing security measures.
- Traditional monitoring tools often provide outdated information from the surface layer of the dark web, rendering it ineffective in preventing timely responses to threats.

TIMELINESS AND SEVERITY OF BREACHES

- Intelligence on data breaches becomes stale quickly, increasing the likelihood of attackers having already exploited the compromised information.
- The recency and severity of breaches determine the urgency for criminals to monetize the stolen data, necessitating real-time monitoring and response capabilities.

MITIGATION STRATEGIES

- A comprehensive view of exposed data and its severity is essential for mitigating the impact of prior exposures and preventing future breaches.
- Real-time alerts enable proactive measures to prevent account takeover and fraud as criminal tactics evolve.

CHALLENGES OF DATA OVERLOAD

- Security teams are inundated with excessive data, hindering their ability to effectively analyze and respond to threats.
- Operationalizing risk insights requires advanced analytics and next-gen threat intelligence that can be integrated seamlessly into existing workflows without adding extra burden on resources.

“Oftentimes the information that we get through SpyCloud comes weeks in advance compared to some of the other platforms out there.”

TOM ALDRICH | CHIEF REVENUE OFFICER
360 PRIVACY

3 False Sense of Security Amidst Emerging Threats

Relying solely on reacting to known threats isn't sufficient. With emerging and constantly evolving threats, organizations must proactively anticipate and adapt to stay ahead of cybercriminals. This is especially crucial in addressing the threat posed by malware, which is rendering traditional security measures ineffective.

CONTINUOUS VIGILANCE AND ADAPTATION

- The dynamic nature of cyber threats requires organizations to constantly monitor the widening gaps in their tech stacks and exposure vulnerabilities across their customer base.
- Strategies must be adaptable to stay ahead of adversaries and anticipate potential attack vectors.

IMPACT OF MALWARE ON SECURITY SOLUTIONS

- Infostealer malware deployments are undermining the effectiveness of conventional account security solutions.
- Previously reliable measures like multi-factor authentication (MFA) are circumvented by malware-exfiltrated session cookies, facilitating advanced account takeover attacks.

SOPHISTICATED ATO TECHNIQUES

- Stolen session cookies are used in anti-detect browsers to execute session hijacking, an advanced account takeover technique.
- This bypasses traditional security measures such as passwords, MFA, and passkeys, highlighting the need for advanced threat mitigation strategies.

"Almost everyone is aware that bad actors are stealing passwords. But I don't think a lot of people realize MFA isn't enough due to the threat of stolen cookies. Session hijacking is still very new – but for Atlassian, it's one of our biggest security priorities moving forward. As long as a cookie stays valid, the gate to that consumer's account remains wide open."

NIELS HEIJMANS | PRINCIPAL SECURITY INTELLIGENCE ANALYST
ATLASSIAN

4 Minimizing Customer Friction in the Digital Experience

Balancing stringent security measures with user experience is a formidable task faced by most teams. This equilibrium is crucial for fostering brand loyalty, customer trust, and optimizing business productivity. However, achieving this balance means navigating the fine line between fraud prevention and customer satisfaction, as any disruptions can lead to lost opportunities. It's imperative for security teams to make informed decisions swiftly without introducing unnecessary friction into customer interactions or operational workflows.

EQUILIBRIUM BETWEEN SECURITY AND USER EXPERIENCE

- Striking the right balance between robust security measures and user-friendly experiences is vital for brand loyalty and business growth.
- Interruptions and friction in the digital journey can result in lost conversions, highlighting the importance of seamless user experiences.

REAL-TIME DECISION-MAKING WITHOUT FRICTION

- Security teams must be capable of making rapid decisions in real-time without impeding customer interactions or operational processes.
- Take action with confidence and ensure a smooth experience for customers while maintaining efficient risk evaluation and mitigation processes.

DIFFERENTIATION FOR TAILORED EXPERIENCES

- Adopting tools that differentiate between low and high-risk users enables businesses to tailor each customer experience appropriately.
- By maintaining low transaction review rates and minimizing the risk of chargebacks and fraud, organizations can drive business forward while preserving customer loyalty and trust.

"Security and usability are often seen as opposites, as tradeoffs. We strive to make sure they aren't. We want to be the most secure and most trusted, but we still want to be the most useful. That's where SpyCloud fits in because it gives us the data we need to intervene when we need to, and then leave users alone when we don't."

HEAD OF OPERATIONS
GLOBAL FINTECH COMPANY

HOW SPYCLOUD SIMPLIFIES CONSUMER RISK PROTECTION FOR BETTER OUTCOMES

SpyCloud Consumer Risk Protection arms your team with insights from the criminal underground, so you can preemptively protect consumers against targeted, automated, and next-generation account takeover attacks. SpyCloud delivers a solution that scales, with outcomes that matter.

Accelerate investigations with robust query results that deliver a full picture of consumer risk

Protect valuable resources by alleviating time and headcount dedicated to darknet data collection, cleansing, and exposure validation

Only **implement friction when necessary** to protect against fraud losses and safeguard consumer identities.

RECEIVE ACTIONABLE INTEL, FAST

With the largest repository of recaptured data of digital identity intelligence in the world, SpyCloud gives you actionable insights on breached credentials, malware-exfiltrated authentication data, and exposed PII – powered by **Cybercrime Analytics.**

SpyCloud's Cybercrime Analytics Engine delivers high volume recaptured data from the deepest layers of the darknet – curating, analyzing, and enriching it with actionable insights to deliver only the most relevant and high quality information to security teams. Businesses can in turn increase operational efficiency by reducing noise and streamlining otherwise manual processes.

- 220+ supported data types tied to a user's digital identity, including sensitive data beyond usernames and passwords – including physical addresses, DOBs, government IDs, IP addresses, credit card numbers, expiration dates, and more
- 90% of passwords available in plaintext
- Enriched details on the recency, severity, and type of exposure

"Our never-ending objective for the team is to reduce alert fatigue, and SpyCloud helps with that. I know if I get a SpyCloud alert, it's actionable."

ANTHONY BRUNSON | SECURITY OPERATIONS MANAGER
LENDINGTREE

GET INSIGHTS THAT DRIVE CONFIDENT DECISIONS

SpyCloud provides a comprehensive view of your customer's risk by analyzing billions of data points exposed in data breaches and malware infections, and correlating them directly to your user – eliminating the guesswork so you can act on what criminals know to protect consumers' digital identities.

SpyCloud's security researchers continuously recapture data at a speed and volume that can't be matched, averaging 25+ billion assets ingested monthly. The data is fresh and actionable, having been recaptured within days of the breach or infection, a stark contrast to existing solutions that often lag behind by 8-12 months post-breach.

Additionally, SpyCloud offers what no other solution on the market can: the ability to identify the highest risk customers whose devices are infected with malware, and the unique authentication data like valid stolen cookies that are in criminals' hands. Identifying and invalidating compromised cookies is a critical component of modern ATO prevention.

90% REDUCTION IN ACCOUNT TAKEOVERS

GLOBAL AIRLINE

AUTOMATE ATO PREVENTION WITH A FRICTIONLESS DIGITAL EXPERIENCE

While SpyCloud maintains the world's largest database of recaptured data, we believe in efficiency, not overload. Our data is curated, stripping away the noise, adding valuable context, cracking passwords, and directly correlating to risk. The result? Actionable insights you can integrate into your decision-making workflows.

Teams can leverage the SpyCloud APIs to implement automated actions like enhanced authentication, password changes, session logouts to invalidate stolen cookies, denying risky transactions, or accelerating low-risk users through their digital journey. SpyCloud promotes a "friction only when necessary" approach to ATO prevention without the constant need for manual intervention.

SpyCloud helps you automate:

- **DARKNET DATA COLLECTION, CLEANSING, PARSING, AND CRACKING**
  SpyCloud collects data other providers can't access, returning only clean and actionable data to aid decision making and tailor the customer journey
- **ACCOUNT TAKEOVER PREVENTION EFFORTS**
  Integrate SpyCloud APIs into your login workflow and preferred tooling to take action when users are exposed
- **SESSION HIJACKING PREVENTION**
  Log users out when their active cookies are stolen from a malware-infected device, preventing authentication bypass and stopping hard-to-detect fraud
- **SECURITY CHECKS**
  Check your customer database on a frequent basis against our continuously updated repository to detect new exposures that put your customers at risk, regardless of if the user has been active

"It just makes it a cleaner experience for the analysts. It's less noise because as an analyst you get fatigue. The beauty of SpyCloud is that you don't get that fatigue because the data is so clean."

CHRIS WINGFIELD | MANAGING DIRECTOR, CLIENT SERVICES
360 PRIVACY

TAILOR THE CUSTOMER JOURNEY BASED ON KNOWN EXPOSURES

Exceptional customer experiences are key to retaining loyalty in a market saturated with options. SpyCloud's underground risk analytics make it easier to tailor the customer journey, balancing a friction-free experience for low-risk users, while high-risk users are flagged for scrutiny or subjected to enhanced authentication or approvals. SpyCloud's data gives your team essential insights, facilitating process continuity, vigilant interaction monitoring, and proactive fraud decisions for a secure and seamless customer interaction.

20M ACCOUNTS RESET

GLOBAL JOB HUNTING COMPANY

BUILD TRUST BY NOTIFYING CUSTOMERS OF EXPOSURES

As a security team, one of your primary responsibilities is to protect customer accounts. But, it's equally important for customers to play their part by adopting better security hygiene. That often requires empowering users through education when their data is exposed.

Notifying customers of third-party breaches, exposed or weak passwords, and malware infections is becoming more common and helps businesses build and foster trust with their consumers, when done the right way. SpyCloud offers best practice guides along with sample messaging your teams can use to notify your customers of potential risks and offer the best guidance on remediation.

"We look at SpyCloud as reputation mitigation as well. You can do everything right and still end up in headlines for the wrong reasons. At a certain volume, ATO is indistinguishable from your platform's security being compromised."

GLOBAL FINTECH COMPANY

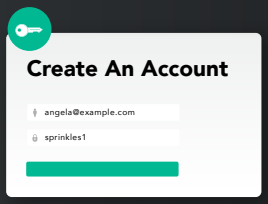
HOW IT WORKS

SpyCloud seamlessly integrates into your account creation, login, and modification flows to help safeguard customer accounts throughout their journey, from start to finish. Our flexible and scalable API is extremely customizable – fluid implementation that offers a manual-free intervention approach, for every stage of your security journey in protecting consumer data and reducing risk to your organization. Here are some examples of what that can look like:

EXAMPLE 1

ACCOUNT CREATION

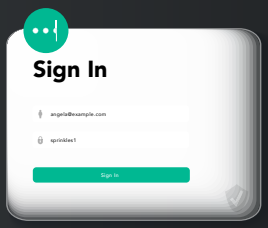
Mary is a new customer creating an ecommerce account. SpyCloud's API detects that the credential combination Mary has chosen was previously exposed in a third-party breach. Mary is prompted to select a stronger password that won't put her at risk of a future account takeover attack.



EXAMPLE 2

ACCOUNT LOGIN

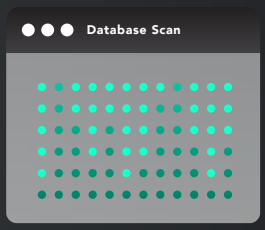
John is an existing customer logging in to his banking account. SpyCloud detects that not only has he been exposed recently, but the origin of the compromise was a malware infection and both his credentials and session cookies were stolen. For high-risk users like John, the organization logs John out to invalidate his active sessions, and forces a password reset to shut down all entry points to his account.



EXAMPLE 3

PROACTIVE DATABASE CHECKS

Organizations often take a proactive approach by regularly checking their entire customer database for new compromises, regardless of the user's activity. They then flag risky accounts for scrutiny of suspicious interactions.



CONSUMER RISK PROTECTION PRODUCT SUITE

SpyCloud product licensing is offered as tiered pricing based on the number of consumer accounts protected.

CONSUMER ATO PREVENTION

Defend against traditional account takeovers by identifying consumers' breach exposures tied to their usernames, email addresses, or phone numbers. Automate password resets for compromised credentials to lock criminals out of accounts.

"We value SpyCloud because not only does it help solve ATO, it gives our team more bandwidth and allows us to provide a better customer experience."

DIRECTOR OF RISK MANAGEMENT
ECOMMERCE MARKETPLACE

VIEW DATASHEET »

SESSION IDENTITY PROTECTION

Stop hard to detect session hijacking attacks by identifying malware stolen cookies used in anti-detection tools to hijack accounts. Invalidate active sessions to prevent undetectable authentication bypass.

"Our customers are everything to us. We have a core value around protecting them at all costs. So by adding Session Identity Protection to the rest of our SpyCloud instance, we basically get rid of the threat of account takeover, whatever the source – which means our customers and their data are safe."

NIELS HEIJMANS
PRINCIPAL SECURITY INTELLIGENCE ANALYST | ATLASSIAN

VIEW DATASHEET »

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.