HUMAN

WHY ACCOUNT SECURITY DOESN'T STOP AT LOGIN

ARE YOUR USERS WHO YOU THINK THEY ARE?

Modern web applications are centered on online accounts. Users may browse as a guest, but they typically have to create or log into an account in order to interact fully with a site or make a purchase.

It is at this crucial login checkpoint that many sites implement username and password forms, CAPTCHA, multi-factor authentication (MFA), security questions, or other verification techniques to determine whether a login is legitimate. However, fraudsters use many different techniques to bypass these defenses and compromise accounts, including using stolen credentials, brute forcing, phishing, malware, and session hijacking.

In many cases, bad actors who successfully log in are free to navigate throughout the account, engage with content, and take any action available to them. This leaves a gap where bad actors can commit numerous types of fraud and abuse post-login. In addition, fraudsters can also create 'fake accounts' that are intended to abuse and steal value from websites and applications. As these accounts are created by the fraudsters themselves, login checks and password resets aren't effective at stopping them.

*Researchers from Digital Shadows estimate that there are **more than 24 billion stolen credentials** available on the dark web.*

ACCOUNTS ARE TARGET-RICH ENVIRONMENTS FOR CYBERCRIMINALS

In an effort to build ongoing relationships with customers and establish revenue retention activities, modern web applications offer and maintain forms of value other than traditional currency. These may include the following, all of which are stored primarily in user accounts:

- Loyalty points
- Digital credits
- Discount codes/coupons
- Airline miles
- Gift card balances
- Free trials

This stored value presents new fraud and abuse opportunities to convert or transfer assets without going through a traditional payment path.

In addition to committing these types of fraud and abuse, bad actors can take fraudulent actions within an account that don't involve the transfer of currency. Some examples:

- Changing the shipping address, email, or password associated with an account
- Disabling MFA
- Reviewing past orders to commit warranty or return fraud
- Capturing stored personally identifiable information (PII)
- Posting positive/negative reviews to influence real users
- Spamming unwanted or malicious content to devalue the experience for real users
- Sharing malware in an attempt to compromise real users' devices
- Sending phishing emails from compromised accounts

Dunkin Brands, Inc. — franchisor of Dunkin' Donuts — ***paid $650,000 in penalties and costs following a credential stuffing attack in which hackers gained unauthorized access to users' accounts****. These accounts held stored value in the form of Dunkin'-branded rewards cards, known as "DD cards," which attackers could have resold online or used to make fraudulent purchases.*

TRADITIONAL FRAUD SOLUTIONS DON'T SEE THE BIGGER PICTURE

Most online fraud prevention solutions focus on two transactional activities: login and checkout. As mentioned earlier, login often includes username and password forms, CAPTCHA challenges, MFA, and security questions.

The second area of tight scrutiny is the checkout, which is when a user actually tries to pay for products or services. At this stage, fraud detection solutions look at payment types or credentials and payment patterns to determine whether the buyer and the payment are legitimate.

While login and checkout are excellent choke points, accounts can be taken over through methods that bypass login and checkout protection (stolen credentials, brute forcing, phishing, malware, session hijacking, etc), and fraud can be committed without going through a typical transaction flow. Solutions focused primarily on login or purchase often miss these creative fraud attempts. This calls for a deeper look at the post-login user's journey as another line of defense to better detect and neutralize compromised and fake accounts.

HOW TO ADDRESS THE POST-LOGIN SECURITY GAP

Addressing this security challenge requires a shift of focus, one in which credential verification is no longer a proxy for identity. Traditional solutions focus on blocking bots and determining payment validity by asking questions such as these:

- Are you a human or a bot?
- Do you have the right credentials?
- Is this credit card number valid?
- Are you trying to rip us off?

While these are good starting questions, they don't actually get at the root of the problem. Instead, they are being used as proxies to answer two more fundamental questions that sit at the heart of account fraud: "Are you who you say you are?" and "Should you be doing what you're doing?"

Just because a user is human doesn't mean they're the human they say they are. Just because a card number is valid doesn't mean that the purchase is valid. Only by establishing user legitimacy can businesses stop account fraud — and simply asking for credentials and serving traditional challenges is no longer enough.

> *According to the 2024 Verizon Data Breach Investigations Report,* ***"68% of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack."*** *If fraudsters get their hands on a valid credential pair, they can easily login and abuse an account.*

APPLY CONTINUOUS MONITORING AND ASSESSMENT

The key to addressing post-login security is applying continuous monitoring and assessment. By continuously evaluating users' post-login activities against behavioral signals, organizations can quickly identify any anomalies that represent instances of account abuse and take action. For instance, if a user accesses account data immediately after login from a new device, this may suggest PII harvesting.

Continuous evaluation can also be used to get a holistic view of activities across all the accounts on a site. For example, website owners might identify a spike in redemptions of free trials across accounts and decide to enforce additional detections in the redemption process to prevent resale of free trials.

By applying a framework of continuous authentication, online businesses can get to the root of the problem of account fraud. This means establishing ongoing attribution and verification of identity and legitimacy across all behaviors.

HUMAN COMPROMISED ACCOUNT DEFENSE

Compromised Account Defense safeguards online accounts by detecting and neutralizing compromised and fake accounts on apps and websites. It stops fraud and abuse, reduces customer risk and cuts your fraud team's workload.

Using behavioral analysis, Compromised Account Defense continuously monitors accounts post-login for suspicious behavior. It generates an evolving risk score based on all activity in an account rather than relying on a single point-in-time check, such as only at login or at the point of transaction.

When a risk threshold is passed, automated customizable responses are triggered. These include calling customer APIs, introducing hard blocks, redirecting to a challenge or to a page that works with an organization's business flow or CIAM. The intuitive management console makes it easy to understand key details of an incident and quickly share data.

Compromised Account Defense is the ideal solution for addressing post-login account security. Learn more at **humansecurity.com**.

"Compromised Account Defense gave us real-time detection with context-aware actions that provide immediate visibility into previously unknown account takeover attacks enabling us to significantly reduce fraud and help desk calls." — CISO AT TOP 3 FREELANCE MARKETPLACE

Sources:

Digital Shadows: Account Takeover in 2022

Office of the New York State Attorney General:

Attorney General James Gets Dunkin' to Fill Holes in Security, Reimburse Hacked Customers

Verizon: 2024 Data Breach Investigations Report

About HUMAN

HUMAN is trusted by the world's leading enterprises and internet platforms to prevent, detect, and respond to cyber attacks with unmatched scale, speed, and decision precision across their advertising, application, and account surfaces. Safeguard your customer journey end to end with complete confidence by consolidating with the Human Defense Platform.