Akamai

Gift Cards Top Wish Lists for Friends, Family, and Fraudsters — Here's How You Secure Them

Gift cards remain the most popular items on wish lists, requested by 61% of respondents in a survey by the **National Retail Federation**. Also a popular target for fraud, gift cards require increasingly sophisticated security, or the experience of giving and getting them can turn from delightful to disappointing. These eight tips will help keep your gift cards safe:

1. Use a Bot Management Solution.

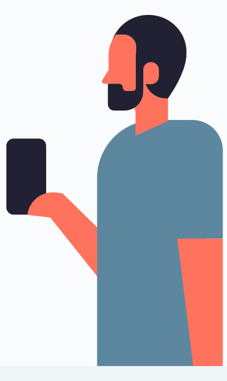
If you allow consumers to check gift card balances online, you need to protect that gift card balance page. Fraudsters use bots to automate the process of going through millions of account number and PIN combinations to find accounts with positive balances and then drain them. All a fraudster has to do is learn the number of digits in the account number and PIN, and then it's off to the races. An advanced bot management solution can identify bot traffic so you can take action.

2. Resist the Urge to Just Block.

When you discover a bot pinging your gift card page, don't rush to block it. Simply blocking bot traffic alerts the operators that you're on to them and spurs adaptations that come back stealthier and stronger. Instead, consider returning deceptive responses that mislead bots. Their efforts will remain harmless to your business, and after enough unsuccessful attempts, they'll move on to pursue more fruitful opportunities.

3. Don't Forget About Mobile.

When curbing gift card abuse, websites are top of mind. But don't forget about mobile apps, or you'll find that, even though the front door is locked, you left the side door wide open. The application programming interface (API) technology that makes native mobile apps more responsive also accelerates the process of querying for information, allowing attackers to check more numbers faster. Bot protection with a mobile software developer's kit (SDK) protects these access points.

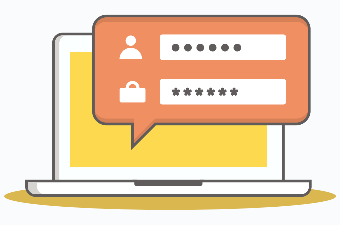


4. Monitor Business Logic.

A web application firewall (WAF) helps secure your site and apps, but unless you also check business logic, you might not notice fraudulent requests. Sophisticated attackers ensure that there is nothing malicious in requests for a WAF to detect. When monitoring business logic, red flags include requests to check the balance of a card that has not yet been activated or number that isn't valid, excessive rate of card failures, and activity from a location inconsistent with your business.

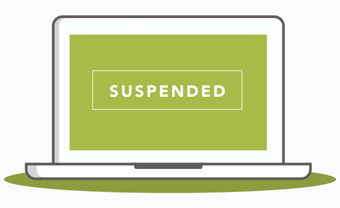
5. Deploy Longer Alphanumeric PIN Combinations.

There's a reason why most websites are now recommending that users create strong passwords for their accounts — passwords with more digits and combinations are harder to break. The same is true for gift card account PIN combinations. With some botnets now exceeding 100,000 unique IP addresses, it doesn't take long to try all the possible combinations for a 4-digit PIN. Using stronger PIN combinations will increase the level of security for every account.



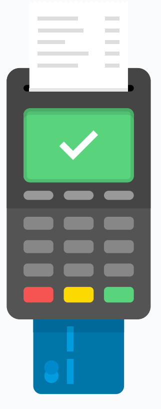
6. Remediate Targeted Accounts.

When you find fraudulent gift card activity, in addition to mitigating the bot problem, take steps to remediate the account. If it's an account behind a login, lock it down and reach out to the owner. Also consider locking inactive gift card accounts in the event of a breach to minimize exposure. For active accounts, request that the card be redeemed in person. While this approach is possibly inconvenient for the customer, the bigger inconvenience would occur if the customer were to find no money left on the card.



7. Check That a Physical Card Has not Been Compromised Before It Leaves the Store.

Sometimes fraudsters aren't hiding behind computers. They might be compromising physical cards in the store — recording the account numbers and removing the scratch-off panels. In these cases, train cashiers to check the integrity of the card before activating it for a customer. If a card looks tampered with, don't put it back on the shelf. Instead, lock down the account and change the PIN before making it available again.



8. Tabletop Your DDoS Runbook to Ensure Operational Readiness.

If customers upload gift cards to a user account before they are redeemed, protect those accounts against credential stuffing so that an attacker doesn't break in and cash out on the value stored. Credential stuffing attacks originate from bots that leverage automation to test multiple thousands of credentials spilled from a data breach, not necessarily your own. A bot management solution helps protect login pages against credential stuffing, too.

With up to 30% of all web traffic traversing its network daily, including some of the largest and most frequently attacked sites in the world, Akamai is uniquely positioned for deep visibility into the constantly evolving attack behaviors of malicious bots. Akamai has the latest bot detection technologies that are proven to identify the most sophisticated bots. With a wide array of advanced and conditional actions to help control the good bots, the bad bots, and the spectrum of bots in between, Akamai can help you manage the impacts of bot traffic to protect your customers, business, and brand.

Learn more about how to manage and mitigate bot threats at **www.akamai.com/bots** or **contact us** to find out how Akamai's advanced bot management technologies can enhance your online security.

Published date: 11/18