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.
   For your gift cards to be a gift that everyone will enjoy, you need to protect gift and balance pages. Frictionless systems enable you to automate the process of giving through millions of account records and PIN combinatios for faster access, with improved business logic and cloud-based deployment. Our 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 the 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 rendering gift card data, be sure to include a portal for mobile. But don’t forget about mobile apps, or you might not secure your business. Too often, the last line of defense is mobile. By being intentional about the security of gift card account numbers and PINs, you’ll safeguard transactions, even when the user’s location is unknown or the device is untrusted.

   A web application firewall (WAF) helps secure your site end to end, but unless you also check business logic, you might lose sight of the forest for the trees. Bot protection with a mobile software developer’s kit (SDK) technology that makes native mobile apps more responsive also accelerates technology that makes native mobile apps more responsive also accelerates.

5. Deploy Longer Alphanumeric PIN Combinations.
   There’s a reason most website administrators use numeric PIN combinations to protect these access points. For their accounts — passwords with more digits and combinations are harder to break. The same is true for gift card account numbers. If you’ve seen 100,000 unique IP addresses, it doesn’t take long to try a list of possible combinations. A brute-force attack on gift card account numbers faster. Bot protection with a mobile software developer’s kit (SDK) technology that makes native mobile apps more responsive also accelerates.

   When you discover fraudulent gift card activity in addition to mitigating the bot problem, take steps to remediate the account. If a bot has learned the account number and PIN combinations to find accounts with positive balances, it’s off to the races. 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 and block traffic so you can take action.

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 implementing physical card theft, fraudsters in retail stores. Don’t let criminals break into and steal your gift cards.

8. Tabletop Your DDoS Runbook to Ensure Operational Readiness.
   In a post-attack state, cybercriminals are no longer content with static websites. They’ve moved on to mobile apps, in a post-attack state. Don’t let criminals break into and steal your gift cards. In a post-attack state, cybercriminals are no longer content with static websites. They’ve moved on to mobile apps, In a post-attack state, cybercriminals are no longer content with static websites. They’ve moved on to mobile apps, in a post-attack state.