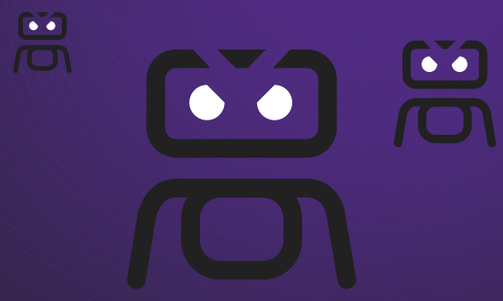
imperva



# How are bad bots contributing to automated fraud?

Bad bots are a major source of online fraud, standing in the way of legitimate customers and creating disruptions across organizations, from marketing to eCommerce and fraud teams. The kinds of automated attacks bad bots perform are only growing in frequency, intensity, and complexity.

## Account Takeover (ATO)

ATO is a form of identity theft through which bad actors attempt to gain illegal access to user accounts belonging to someone else through brute force techniques, mainly Credential Stuffing.

65% of people reuse their passwords, which means as soon as one account is taken over, their other accounts using the same password are also at risk. Both individual users and businesses see negative impacts from successful ATO, from financial fraud to supply-chain issues.

## New Account Fraud

Bad actors use bad bots to create new accounts automatically in massive amounts, generating an army of fake user accounts to commit online fraud, from comment spam to money laundering.

## Credit Card Fraud

The most common types of credit card fraud are card cracking and carding, both of which leverage bad bots. Credit card fraud can negatively impact one's credit score and damages the fraud score of affected businesses.

**Card cracking** uses bots to spread its guesses of a cardholder's CVV number, expiration date, and postal code across multiple websites.

**Carding fraud** occurs when criminals run thousands of small purchases to verify stolen card numbers, then resell verified card info to organized crime rings at a much higher price

## Gift Card Fraud

Also known as Gift Card Cracking and Gift Card Enumeration, gift card fraud is becoming more prevalent as bad bots find gift cards with unused balances and sell the gift card numbers on the dark web for an easy profit.

## Spamming

Fraudulent activity is on the rise in the form of spamming. Bad bots flood the internet with spam comments and can spread fake news and drive users to dubious websites.

## Client-side Attacks

Client-side attacks occur when fraudsters inject malicious JavaScript into the code used on legitimate websites. They can then collect sensitive user information every time a customer fills out a form, from the login page to a purchase order page.

Contact us now to schedule a demo or begin a free trial

**imperva.com**