sift

Q2 2022 DIGITAL TRUST & SAFETY INDEX

Quantifying the collateral damage of content fraud

Contents

ONLINE SCAMS

The Surging Epidemic Plaguing Digital Commerce

It's been a banner year for online scammers. From Ukrainian fundraising and COVID-19 relief scams to romance and crypto cons, content abuse is gaining major momentum among fraudsters. Used as a means to a financial end, content fraud in the form of scams, spam, misinformation, and phishing is increasingly being used as a tool to swindle consumers on seemingly trustworthy sites. Across Sift's global network, we've seen significant increases in blocked content fraud over the past year, signaling rising fraud that undermines community integrity and kills growth across the board.

The average rate of fraudulent content blocked by Sift rose by nearly one-third between Q1 2021-Q1 2022.

Unleashing spam is rarely the end goal for fraudsters. Ultimately, these scammers are money motivated. They use deceptive content as a hook to phish for personal information, usernames, and passwords in order to take over accounts and commit financial crime. The stolen information is later sold on the deep or dark web for profit, or used first-hand to steal rewards, use store credit, and transfer funds.

In this report, we investigate how cybercriminals use content as a vehicle to commit widespread fraud impacting various industries. These findings draw from Sift's global data network representing over 34,000 sites and apps, as well as responses from 1,100 consumers surveyed in April 2022*.

Fraudsters Double Down on Online Scams

62% of consumers encounter scams more frequently than any other type of fraudulent content.

When fraudsters find a fruitful fraud vector, they launch all-out attacks to reap maximum profit—precisely what we're seeing with online spam and scams. The rise in digital transactions, coupled with inflation and pent-up demand, has created prime conditions for an epidemic of content fraud. For many businesses, content abuse is one of the most challenging forms of fraud to fight, often involving considerable time investment from trust and safety teams.

Scams make up over half of content blocked by Sift**

Scams	**55.3%**
Spam	30.4%
Toxic	13.9%
Commercial	0.03%

***For detailed descriptions of fraudulent content types, see Sift's public documentation.*

**On behalf of Sift, Researchscape International polled 1,100 adults (aged 18+) across the United States via online survey in April 2022.*

2022 Emerging Industry Trends & Consumer Insights

Fraudsters are devising more sophisticated, automated tactics to broaden the scale of their attacks. Recent reports of text scams, fake ads, social media scams, and phony job opportunities have flooded the news. Thanks to convincing impersonations, fraudsters are able to deceive consumers into believing they're trustworthy—at least long enough to extract the compromising information they seek.

Being accosted by fake and false content on a near-daily basis can be financially and emotionally debilitating for consumers, with more falling victim to these online scams than ever before. The Federal Trade Commission (FTC) reported consumers lost a record-breaking $5.8 billion to fraud in 2021, a 70% increase from the previous year, most commonly from imposter fraud and online shopping scams.

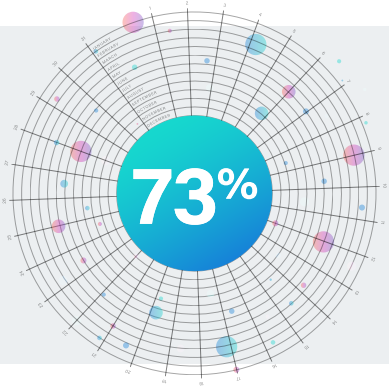
Exposure to Fraudulent Content Leads to Brand Abandonment

of consumers would stop using a website completely if they encountered fake or misleading content.

Relying solely on users to flag suspicious content isn't enough to uphold the safety of online platforms—the responsibility falls on merchants, and the stakes are high. The prospect of losing nearly 70% of customers victimized by scams poses a gut-wrenching threat to any business. But smaller businesses may bear the brunt of the damage, as they lack the clout and stickiness of household-name brands.

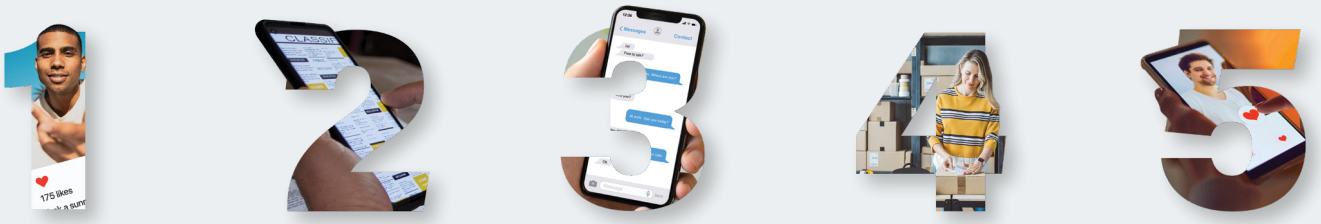
It's crucial to take into account the true cost of content fraud, as it has the potential to cause major customer churn. A brand's reputation sits precariously on the shoulders of even one ill-willed message or link, potentially causing lasting damage. Companies must take into account customer acquisition cost (CAC) and lifetime value (LTV) to quantify how losing a loyal customer could harm the business.

Fraudsters see communities and social sites as playgrounds for profit, using the platforms as a low-cost way to reach billions of victims. Lining up with Sift network data, the FTC found social media was the most common and profitable way for scammers to con consumers in 2021. Last year, more than 95,000 people reported $770 million lost to fraud initiated on social media platforms—a staggering eighteenfold increase from 2017 reported losses.



Nearly three-quarters of respondents see misleading content or false information daily or weekly.

Consumers Say: Social sites and communities among the spammiest and scammiest places online*



65%
Social networking sites

30%
Classifieds

30%
Messaging apps **

28%
Marketplaces

22%
Dating sites

** Respondents could select multiple options.*
*** Not including SMS and native messaging apps.*

Cybercriminals Capitalize on the Crypto Craze

Fraudsters are increasingly leveraging direct messaging to lure users with too-good-to-be-true crypto investments. Despite the recent downturn, the crypto market value is hovering around $1 trillion, and fraudsters are flocking to cash in on the still lucrative potential. These cybercriminals are taking advantage of the absence of formalized regulations, low consumer awareness around online security, and lack of fraud controls to deploy fraudulent content. Case in point: Chainalysis reported crypto scammers took home a record $14 billion in cryptocurrency in 2021, a 79% increase from 2020.

Our recent survey reveals how pervasive crypto scams have become online and the alarming number of consumers who have lost money to these scammers. Respondents report encountering these scams most commonly on social networking sites, marketplaces, gaming sites, and dating apps, but they're also beginning to emerge on other sites as well. And the targeted generations skew younger, with more than one in two Millennials and Gen Zers encountering crypto scams online.

Crypto Cons Are Ubiquitous

43%

Nearly half of consumers have encountered scams asking them to join crypto exchanges.

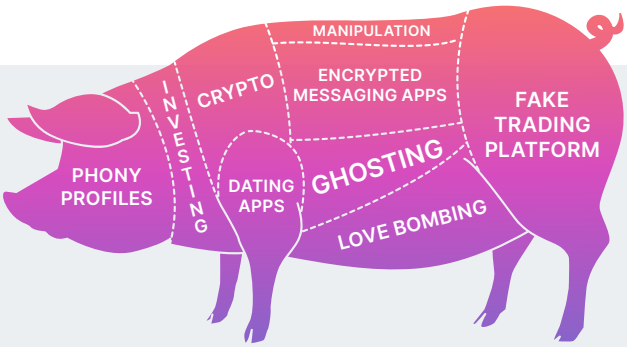
Consumers Are Losing to Crypto Scams

22%

More than one in five consumers who have encountered crypto scams have lost money.

JANE LEE *Sift Trust and Safety Architect*

Fraudsters are treating cryptocurrency as a free-for-all, exploiting the perfect storm of industry growth, lagging regulations, and the lack of consumer education.



Pig Butchering Scam Couples Romance with Crypto

Another toxic fraud trend combines romance with crypto investing. Sift Trust and Safety Architect Jane Lee recently went undercover to reveal the anatomy of the Pig Butchering scam, in which scammers lure online daters to invest in fake crypto exchanges. These fraudsters are highly-skilled professionals with extensive technological sophistication, and it's up to merchants to protect consumers and keep these ill-willed actors at bay.

JANE LEE, *Sift Trust and Safety Architect*

Businesses can't keep turning a blind eye to content abuse. Catching scams on one platform could prevent downstream disasters involving account takeover and financial theft on countless other sites.

Combatting Content Fraud with Digital Trust & Safety

Although content abuse has disproportionately impacted communities and social sites this past year, the ramifications of these scams don't end there. In the global interconnected network of the Fraud Economy, content abuse affects everyone. It only takes one successful phishing scheme to create a domino effect, leading to tarnished brand reputation, compromised user credentials, ATO attacks, and payment fraud. Downstream, content fraud has the potential to cause destructive collateral damage on sites and apps across a wide range of industries. Most merchants don't have the tools to get ahead, or they rely on manual solutions and reactive rules that are ineffective and add friction to trusted users.

The only way to effectively prevent fraudulent content is by adopting solutions that optimize speed, accuracy, and automation. Trust and safety teams need to be equipped to track patterns and user behavior with machine learning (ML) to combat every type of fraud and abuse. By investing in a holistic and flexible solution, companies can stop fraud before account creation and catch content abuse faster, all while building trust among legitimate users and catalyzing growth.

Proactively prevent all types of fraud with Sift

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents fraud and abuse with real-time machine learning that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including Twitter, Wayfair, and Doordash rely on Sift to catalyze growth and stop fraud before it starts. Visit us at sift.com or follow us on LinkedIn.

Access our previous Digital Trust & Safety Index reports on our website and explore the latest fraud trends on our Fraud Intelligence Center.