CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

November 22, 2023

As Black Friday Approaches, 3 Key Trends Offer Insights for Mitigating Online Shopping Scams

Executive Summary

As Black Friday approaches and the holiday shopping season begins, scammers are likely to intensify their operations, as indicated by a 22% increase in consumer scam losses during 2022 Black Friday and Cyber Monday sales. Insikt Group analyzed recent high-impact scam website campaigns to identify 3 key themes in how scammers operate their websites, why, and how consumers and businesses can use these findings to protect themselves.

Scams are a growing threat, with reported US losses ranging from $8.8 to $10.3 billion in 2022. Online shopping scams present financial fraud risks for consumers, financial institutions, and payment processors. They also raise risks of brand impairment by undermining consumer trust in the businesses they impersonate: a 2023 study indicated that 19% of shoppers had abandoned their shopping cars because they didn't trust the website to keep their payment card data secure. Moreover, businesses likely suffer indirect financial and reputational damage from online shopping scams due to lost potential revenue and consumers' perception of businesses' inadequate responses to scams that leverage the businesses' brands.

Scam website campaigns are grounded in social engineering and necessarily depend on scale for success. Therefore, businesses should view 3 strategies — identification, analysis, and customer awareness — as cornerstones for scam prevention, with the solicitation of scam website leads from customers serving as a crucial bedrock for these strategies. These mitigation strategies are likely to reduce the aggregate financial risks posed by scam websites at the cost of increased investment in research, with businesses best served by an approach tailored to their needs. Specifically, increasing customer awareness of scams would likely yield benefits for all businesses, incurring only marginal increases in existing operating costs associated with customer communications management, whereas increased investment in scam campaign identification and analysis would likely only yield substantial benefits for financial institutions, major digital retailers, and other businesses in the e-commerce and payments industries. Looking forward, generative artificial intelligence (AI) will likely amplify the threat posed by scam websites by lowering barriers to entry for scammers, whom AI will empower to swiftly generate content for scam websites and ad lures.

Key Findings

- As shoppers look for holiday deals on Black Friday, scammers will exploit the opportunity to profit using scam e-commerce websites and phishing pages.
- Scammers craft their websites using cookie-cutter methods and open-source tools, allowing them to scale up their operations but providing businesses with a potential means of detection.
- While scammers widely use open-source tools to create their scam websites, they also employ sophisticated methods to disseminate their scams, cash out victims' payment cards and crypto wallets, and steal victim data.
- Scammers understand and exploit consumer psychology to maximize the impact of their scams.

Methodology

This report's findings are grounded in an analysis of evidence from dark web sources and a meta-analysis of sophisticated scam campaigns analyzed by Insikt Group since 2020, including:

- A **China-based scam** e-commerce website campaign consisting of 560 domains that stole victims' credit card data (2020)
- Various **cryptocurrency scam** schemes that use "crypto drainer" scripts to steal crypto assets (2023)
- A **subscription scam** campaign consisting of 348 domains (2023)
- A **smishing campaign** that distributed text messages containing links to scam pages modeled after the websites of the US Postal Service (USPS) and other nations' postal services across 543 domains (2023)
- A network of **201 scam domains** that were likely operated by the same threat actor(s) (2023)

More broadly, the findings in this report are also supported by open-source reporting and the extensive experience of Insikt Group's Payment Fraud Intelligence (PFI, formerly Gemini Advisory) in identifying and researching fraud threats on both dark web and open sources.

Threat Analysis

Scams — particularly scam websites posing as legitimate e-commerce shops — are a growing threat. In February 2023, a business blog article from the US Federal Trade Commission (FTC) indicated that consumers had reported losing almost $8.8 billion to scams in 2022, a 30% increase from 2021. The US Federal Bureau of Investigation's (FBI) Internet Crime Center (IC3) reported even higher losses for online scams in 2022: $10.3 billion. In an October 2023 data spotlight, the FTC revealed that online shopping scams were the most commonly reported social media scams between January 2023 and June 2023, accounting for 8% of all reported financial losses from social media scams in that time. This figure, combined with the data spotlight's reported $2.7 billion in social media scam losses since 2021, suggests that consumers may have lost as much as $216 million to online shopping scams since 2021. In reality, scam losses are likely even higher: the FTC's estimates only account for losses that consumers and law enforcement reported through the Consumer Sentinel Network.

The impact of the online scam threat is more than just the sum of victims' direct financial losses. As indicated by the FTC, each dollar lost to fraud is a dollar lost to legitimate business, and widespread online scams likely increase both consumer skepticism toward digital advertising and consumer aversion toward purchases on unfamiliar e-commerce websites. A 2023 study by Baymard Institute, a web user experience researcher, indicated that 19% of shoppers abandoned their shopping carts due to a lack of trust that a website would protect their payment card data. Additionally, a 2021 trust survey by Mimecast, a brand protection provider, found that 61% of consumers would lose trust in a brand if they fell victim to a scam website impersonating that brand. The same survey indicated that refusing to take

responsibility for cyberattacks leveraging a business's brand or reimburse victims were the 2 biggest factors negatively impacting brand reputation.

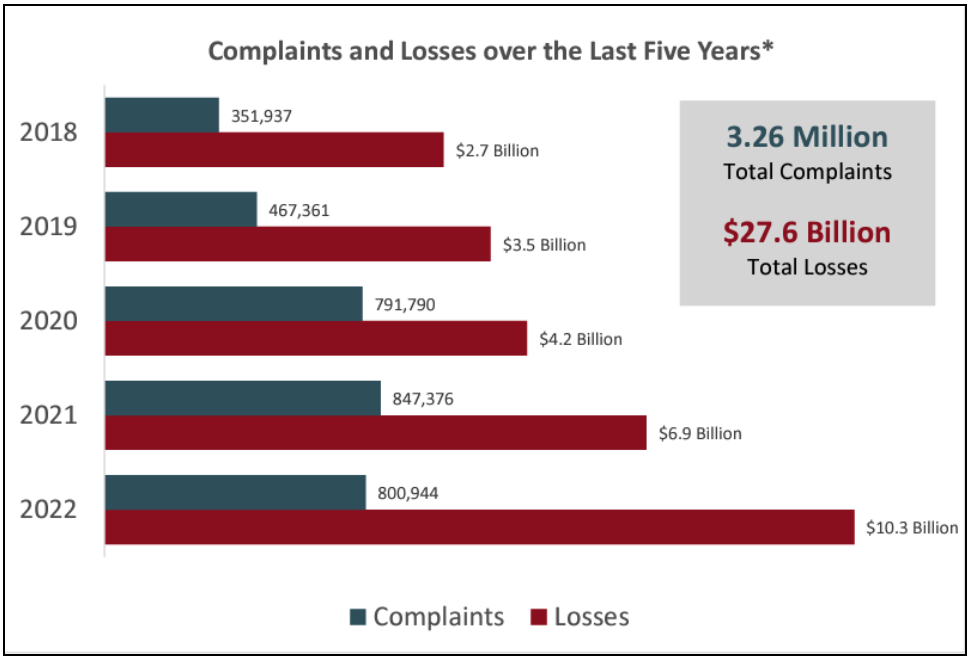


Figure 1: *IC3 has reported rising losses from online scams each year since 2018 (Source: FBI IC3 Internet Crime Report 2022)*

With Black Friday approaching, consumers are looking for online bargains, and opportunistic scammers are likely to capitalize. On November 8, 2023, Barclays warned that purchase scams cost shoppers 22% more in losses during Black Friday and Cyber Monday sales in 2022.

To help online shoppers protect their wallets — as well as the companies who stand to lose out on business when scam victims' money is stolen — Insikt Group has analyzed recent scam website campaigns. We identified 3 key themes in how scammers establish and operate their fraudulent e-commerce shops, why they use these tactics, and what those patterns and trends offer potential victims and legitimate businesses in terms of recognizing, avoiding, and mitigating the threat posed by online scam websites.

Figure 2: *Insikt Group's analysis of scam website campaigns revealed 3 key themes in how scammers establish and operate scam websites, why they use these tactics, and what these themes mean for victims and businesses (Source: Recorded Future)*

"Cookie-Cutter" Website Creation Allows Scammers to Ramp Up Operations — and Provides Businesses with Potential Means of Detection

Like most scams, the success of scam e-commerce websites is largely a function of quantity, not quality. Whether fraudsters aim to monetize their fake e-commerce websites through fraudulent transactions on linked merchant accounts ("scam pages") or through the resale of data that has been stolen via phishing tactics ("phishing pages"), they all generally seek to capitalize on the sheer volume of their scam websites. As a result, scammers often repeatedly use the same domain registrars, open-source tools and platforms, and more to create and configure their scam websites.

For fraudsters, this approach is sufficient. Unlike legitimate e-commerce merchants, scammers have no need for the secure or robust backend web infrastructure typically provided by premium third-party

services. Fraudulent e-commerce stores only require bare-bones backend functionality to defraud victims, safeguard little or no sensitive data, and tend to be short-lived. As a result, the emphasis on quantity over quality offers scammers the scale they require with few material drawbacks — and still enables the scammers to create polished, appealing fake e-commerce stores capable of luring unwary victims.

Domain Registration and Network Infrastructure

Typically, a scammer will rely on the same domain registrars and network infrastructure to establish and operate their scam websites. Many of the scam campaigns we analyze indicate that the websites within a single campaign tend to share overlapping domain registration information and IP addresses.

For example, 280 out of 328 domains used by the subscription scam we analyzed were registered to a single domain registrar. Payment subdomains containing checkout functions on these 280 domains shared the same 8 IP addresses, a ratio of 35 subdomains per IP address. Meanwhile, the network of 201 linked scam domains that we identified contained 147 domains — 73% of the domains in the network — that were registered via a single China-based domain registrar. All 201 domains were operated from 20 IP addresses, a ratio of approximately 10 domains per IP address.

Website Configuration

At the same time, scammers use free solutions to harden and configure their scam website infrastructure. Scam campaigns often use Cloudflare, a content delivery network, to mask their home pages' IP addresses. They also use OpenCart, an open-source e-commerce management system that offers shopping cart functionality, to configure their fraudulent online stores. When necessary, scammers also use bot application programming interfaces (API) for Telegram, a free messenger, to exfiltrate stolen data. We have previously encountered this tactic with Magecart e-skimmer infections[1] and delve into greater detail on its use below.

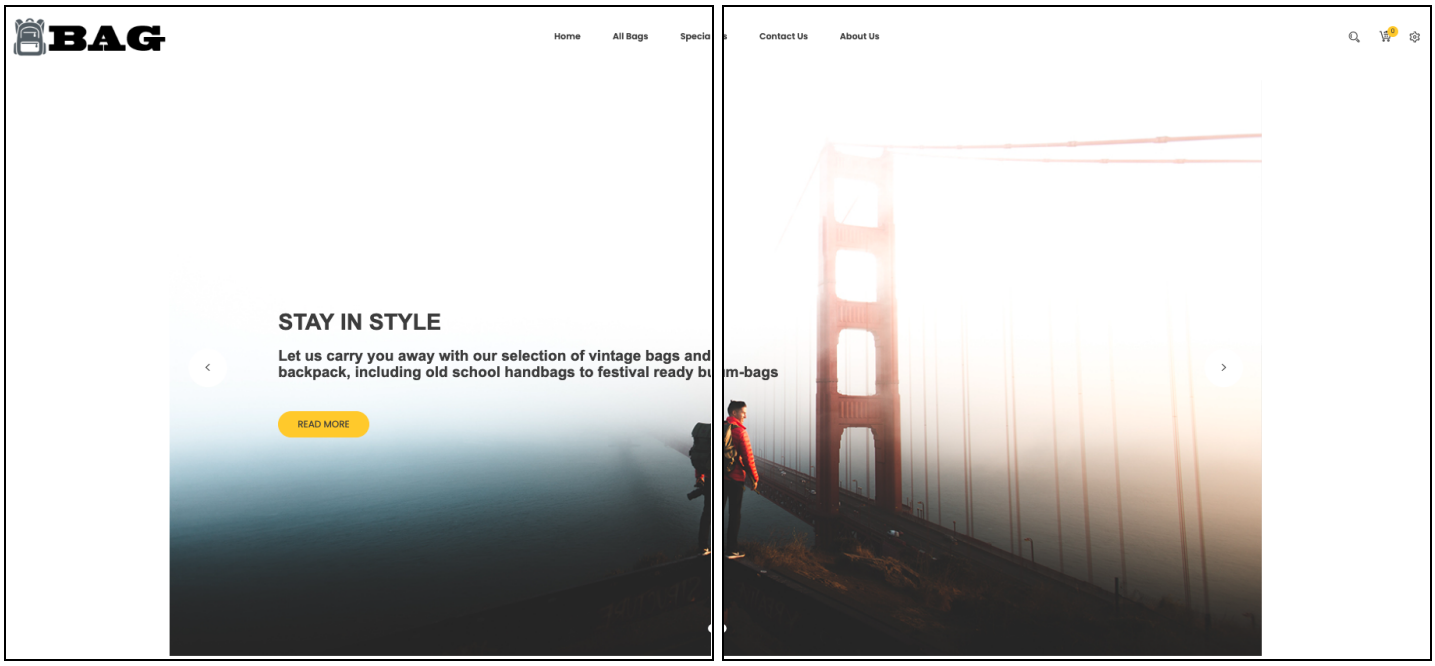
Besides the tools and services mentioned above, other website configuration elements recycled within scam campaigns include:

- **LiveChat widget license numbers:** The subscription scam reused a single LiveChat widget license number across its scam domains.
- **Google Analytics codes:** The USPS-based smishing campaign distributed links to scam pages that used the same Google Analytics code present on the official USPS website. The China-based scam campaign's domains also used shared Google Analytics codes.
- **Facebook Pixel identifiers (IDs):** As with Google Analytics codes, the China-based scam campaign used overlapping Facebook Pixel IDs.

[1] Unlike scam websites, fraudsters use Magecart e-skimmer infections to steal data from legitimate e-commerce websites. Scam websites are built from the ground up to support fraud.

Website Design and Content

When it comes to website design, scam website operators recycle the same content and design elements, even among purportedly different scam websites. For the China-based scam website campaign, we determined that the scam operators reused the same 7 templates, image files, and the text of their "About Us" pages across all of their scam domains. Similarly, the subscription scam campaign we identified reused identical Terms of Service across each of its domains.



Figures 3 and 4: *These 2 scam websites both used identical designs and were linked to fraudulent credit card transactions (Source: Recorded Future, partner financial institution)*

For scammers, the advantages of a quantity-over-quality approach are viability and scale. Reusing free, openly accessible tools allows scam operators to swiftly increase the scale of their scam operations. For example, the subscription scam operators registered dozens of domains in short bursts of time — as many as 19 within 1 minute — as part of a concerted effort to expand the scale of their campaign. Advantages to scale aside, part of the underlying logic as to why threat actors use cookie-cutter approaches to expand their scam infrastructure may also lie in their reliance on monosourced "fraud-as-a-service" offerings common in the dark web cybercrime ecosystem, which we describe in greater detail below.

For all the strengths that open-source tools and scalable, cookie-cutter designs offer scammers, the overwhelming similarities that arise between related scam websites also create an opening for researchers and businesses to identify networks of related scam websites. This can be done by identifying common elements or tools used to create a single scam website — for example, the tools and elements described above — and then extrapolating them in an expanded search.

Takeaways: Scam e-commerce websites rely on scale to maximize profit. This means that scam websites operated by the same threat actors usually reuse the same elements and tools to create more scam websites. By identifying these elements, businesses and researchers can identify related scam websites. Where there's one scam website, there's almost certainly more.

Scam Operators Use Advanced Methods to Disseminate Scam Websites, Cash Out Victims' Payment Cards, and Steal Victim Data

Since e-commerce scam operators reuse free infrastructure, content, and website designs, one would be forgiven for assuming their tactics must be primitive. Our analysis has shown the opposite to be true: e-commerce scam operators use sophisticated methods to disseminate scam websites to victims, cash out victims' payment cards, and steal victim data. Meanwhile, third-party "fraud-as-a-service" offerings from other cybercriminals on the dark web allow scammers to implement these operations at scale.

Dissemination: Scammers Exploit the Online Advertising Ecosystem to Maximize Exposure

Since scammers rely on quantity over quality for their scam websites to profit, dissemination is perhaps the most crucial element for a scam campaign's success. According to the Australian consumer advocacy group CHOICE, "Scams are often sophisticated operations run like businesses, and they're using the same tools that legitimate businesses use to advertise". To this end, scammers take advantage of the online advertising ecosystem — particularly on search engines and social media — to cast as wide a net as possible with their scam websites, ensuring maximum exposure.

The use of online advertising to distribute malicious content, including scam websites, is known as malvertising. To enhance the effectiveness of malvertising attacks, threat actors use specialized techniques such as SEO poisoning. To avoid detection while advertising, scam operators use cloaking techniques, which present different content to ad verification systems than they do to victims, ultimately allowing the malvertising to go unnoticed. Insikt Group previously reported on threat actors' use of the online advertising ecosystem to support illegal activity in November 2023.

Dark web sources indicate that cybercriminal advertisers and publishers frequently cooperate as part of an intricate dark web ecosystem to distribute malvertising attacks, including for scam websites. In this arrangement, the "advertisers" — scam operators intent on disseminating scam websites — purchase ad inventory from the "publishers" — fraudsters with access to compromised or fraudulent advertising accounts on major ad platforms. These fraudster-publishers abuse the compromised or fraudulent advertising accounts to purchase legitimate ad inventory for scam-advertisers. To pay for this malvertising, the fraudster-publishers use stolen payment information (including credit cards, bank accounts, and more) linked to the compromised or fraudulent advertising account. Given that scam websites can be used to compromise victim payment cards or online banking credentials, this attack vector also indirectly sustains a "vicious circle" of fraud.

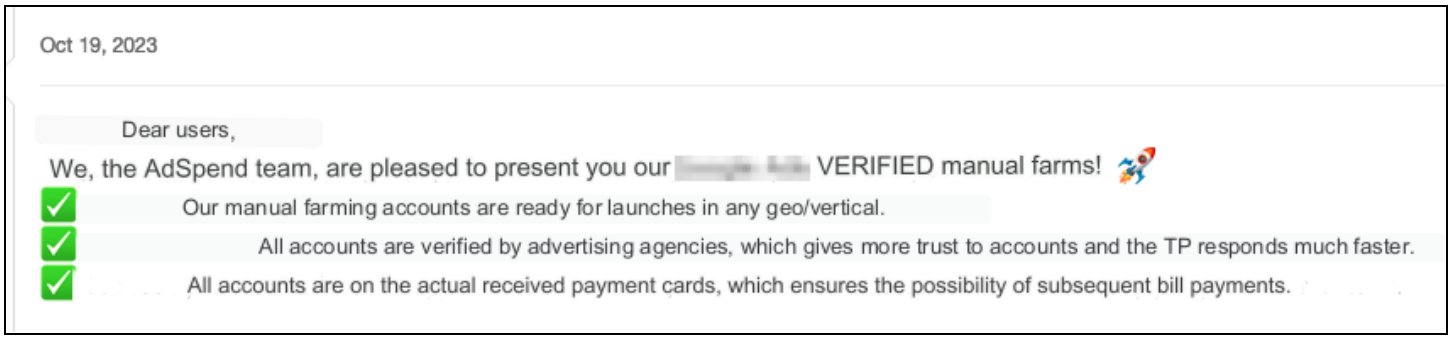


Figure 5: *A threat actor offered to sell access to online advertising accounts, which scammers can use to disseminate their scam websites via malvertising tactics (Source: Top-tier dark web forum)*

Despite scammers' reliance on the legitimate online advertising ecosystem to disseminate their scam websites, the advertising technology ("ad tech") companies that facilitate online advertising are unlikely to implement solutions to reduce malvertising for 2 reasons. First, threat actors' use of sophisticated cloaking techniques complicates malvertising detection and prevention. More importantly, however, misaligned incentives discourage ad tech companies from preventing malvertising attacks. Most ad tech companies earn money from online ads regardless of whether the ads are legitimate or malicious.

Takeaways: Consumers and businesses should be skeptical of social media- and search engine-enabled online advertising, which is rife with poisoned malvertising ads. In a December 2022 alert, IC3 went so far as to recommend consumers use ad blockers to protect themselves.

Cash-Out: Merchant Accounts and Clever Payment Strategies Allow Scammers to Monetize Cards

For online shopping scams to be successful, scammers must have a means of obtaining payments from their victims. Often, this takes the form of electronic payments that are common for online e-commerce transactions. To facilitate online payments for bogus goods and services, scammers often connect their scam websites to fraudulent or compromised merchant accounts, which can be acquired from dark web sources (Figure 6).

Scammers' employment of these merchant accounts is varied based on their resources and needs. Our analysis of 201 linked scam domains suggested the scam website operators may have rotated their merchant account infrastructure as older domains "aged out" and new, fresher domains were registered. The earlier China-based scam campaign, however, prioritized durability. Merchant accounts linked to the China-based scam websites were individually linked, with second-level domain names present in the scam websites' linked merchant names. Links between these scam domain and merchant name pairs were unique in order to obscure relationships with other domains and merchant accounts within the scam campaign's infrastructure.

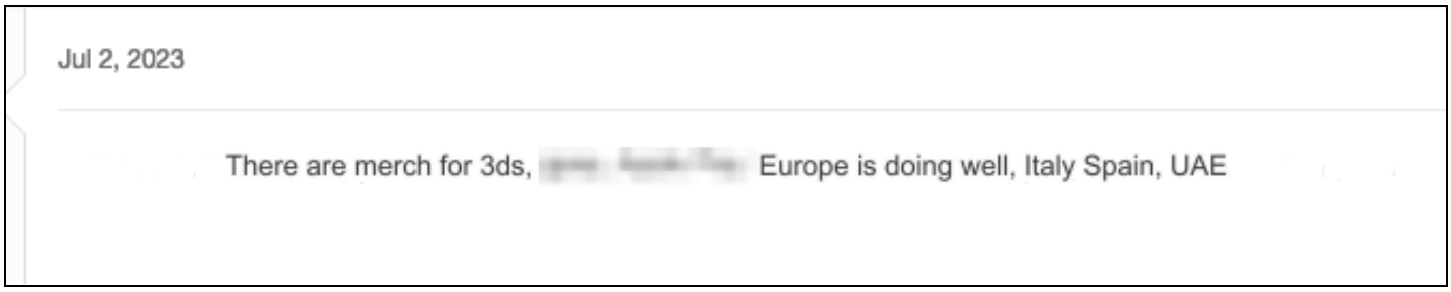


Figure 6: *A threat actor advertised available merchant accounts to monetize victims' payment cards, which threat actors can link to scam websites (Source: Top-tier dark web forum)*

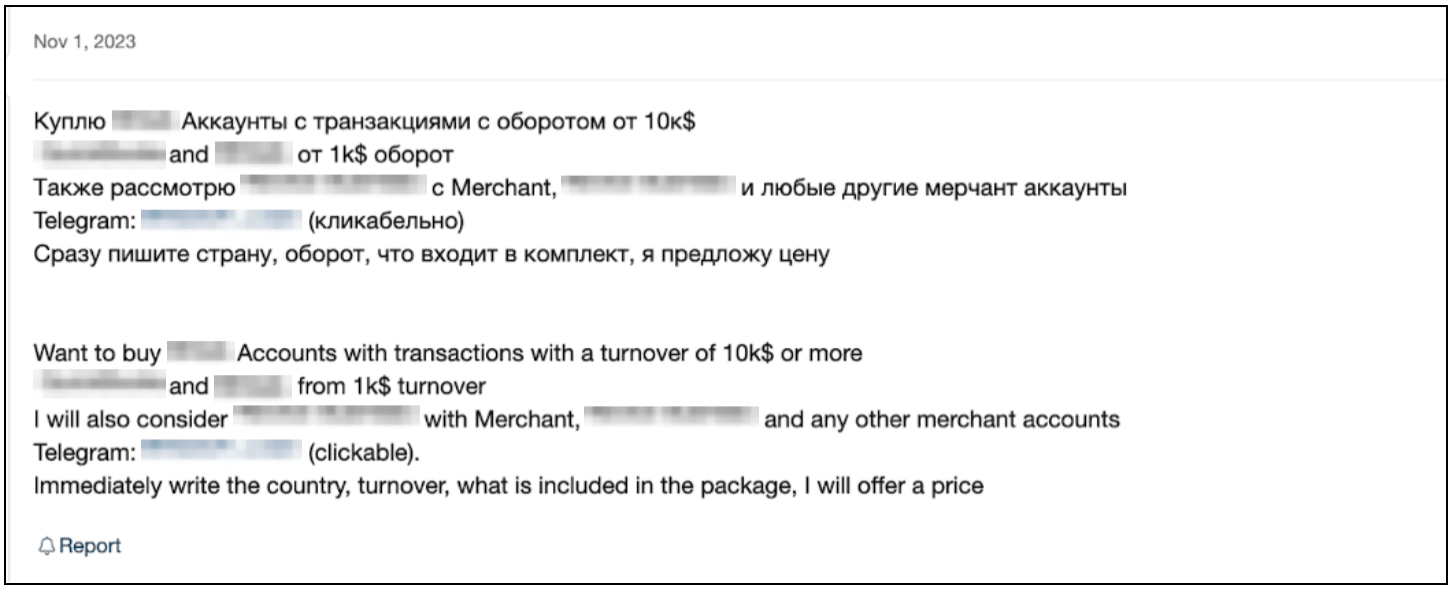


Figure 7: *A threat actor requested to purchase merchant accounts, likely for fraud or other illegal activity (Source: Top-tier dark web forum)*

Use of merchant accounts does not guarantee that a scam website can successfully steal from victims. Financial institutions — in particular, card issuer banks — use advanced anti-fraud technologies to detect and prevent payment fraud when possible. Fraud detection algorithms compare a host of indicators, and pattern recognition techniques allow financial institutions to identify blocks of suspicious merchant accounts (as indicated by merchant acquirer and merchant ID patterns, for example) that indicate scam activity. When scams result in financial losses, chargebacks can also allow victims to recover lost funds from scam-connected merchant accounts, ultimately increasing operating costs for the card issuer.

Scammers operating scam e-commerce websites have devised ingenious methods to ensure that monetization through linked merchant accounts goes off without a hitch. In particular, the subscription scam charged European customers an initial sign-up fee for a bogus subscription-based service, effectively establishing a transaction history. Within days, the scam websites charged subscription fees of €49 to €69 as part of their main cash-out mechanism. This "low-to-high" transaction tactic exploits the different sets of rules that anti-fraud technology commonly uses to monitor card-on-file charges.

Scammers using this tactic can likely bypass strong customer authentication (SCA) — for example, 3D Secure 2.0 (3DS2) — which European regulators only require when payers create, amend, or initiate recurring payments. In effect, if a scam website successfully elicits a smaller initial payment from a victim, the larger follow-up payment is easier to push through. These tactics are likely effective against both European customers and more broadly, including in the US.

An increasing number of cryptocurrency-based scam schemes have also emerged in recent years, and the threat actors operating these scams combine both technical and social-engineering skills to steal victims' assets. Since April 2022, we have observed threat actors deploy cryptocurrency drainers via numerous attack vectors, including airdrop scams, pig butchering scams, and phishing pages that target trusted cryptocurrency exchanges. Within the cryptocurrency and non-fungible token (NFT) space, the sale of stand-alone drainers is commonplace and frequently advertised across dark web forums and marketplaces.

Airdrop scams and pig butchering scams involve social engineering and are typically deployed via phishing campaigns targeting unsuspecting cryptocurrency users:

- In an airdrop scam, threat actors often claim they are launching a new cryptocurrency or NFT and offer to give free coins or NFTs to new adopters under the pretext of building a user base (Figure 8). These giveaways imitate legitimate airdrop marketing strategies. To accept these assets, scammers direct victims to access a malicious link. Once the victim accesses the link, a clipper or drainer will be deployed onto the victim's cryptocurrency wallet and begin stealing funds.
- In a pig butchering scam, fraudsters seek to convince unsuspecting victims to connect their wallets to lend funds for the purpose of liquidity mining, a legitimate process that sees users lend crypto assets to a cryptocurrency exchange in return for rewards. Although the victim will initially see returns on their investment, after the threat actor has gained the victim's trust, they will deploy a cryptocurrency drainer and steal the victim's funds.

Many drainer-based scam schemes specifically abuse cryptocurrencies based on Ethereum Request for Comment 20 (ERC20). ERC20 is a standard set of guidelines that govern the Ethereum blockchain, including coins, smart contracts, and NFTs. Drainers also often abuse the "set approval for all" (SAFA) function, which grants smart contracts, NFTs, and ERC20-based tokens permission to transfer from a user's wallet at a future time. The SAFA function is intended to enhance user experience by reducing the need for repetitive approval requests when executing wallet transactions.

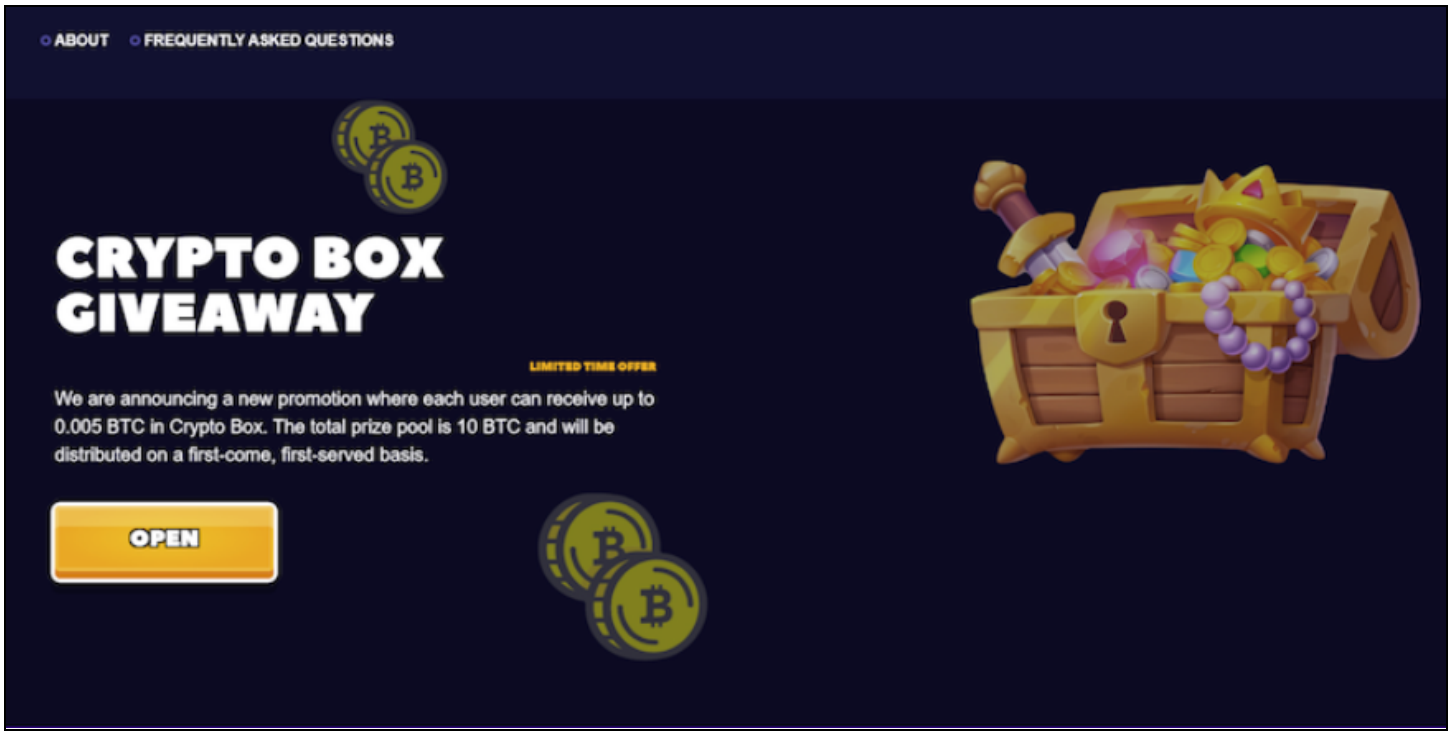


Figure 8: *Airdrop scam phishing pages purport to offer free cryptocurrency (Source: Top-tier dark web forum)*

Takeaways: Merchant accounts associated with numerous complaints of reported scam transactions should be flagged as fraudulent. Research into common elements between scam merchant accounts — for example, merchant acquirer bank identification numbers (BINs) and merchant category codes (MCCs) — could allow banks to surface blocks of related scam merchant accounts, which can be used to raise risk scores for automated fraud prevention systems. For crypto scams, wallet clustering techniques can help researchers and businesses trace stolen crypto assets.

Data Theft: Scammers Use Merchant Accounts and Telegram to Steal Card Data for Dark Web Resale

In addition to cashing out victims' payment cards through direct transactions on linked merchant accounts, scam websites usually allow scammers to obtain victims' personal and financial data to sell on the dark web. Scam websites with payment functionality and linked merchant accounts can inherently steal victim card data. Other scam websites use phishing tactics to steal data, which they must exfiltrate in an easily manipulable form.

The smishing campaign modeled after USPS used a Telegram bot API to exfiltrate stolen victim card data and personally identifiable information (PII) from linked scam websites. Bots are essentially scripts capable of performing repetitive actions. After the campaign's victims submitted their data to the scam website, the scam website transmitted the data to one of several exfiltration domains and a Telegram bot API. "@chenlun", the threat actor responsible for operating this domain, later shared curated selections of the stolen data in a separate Telegram channel.

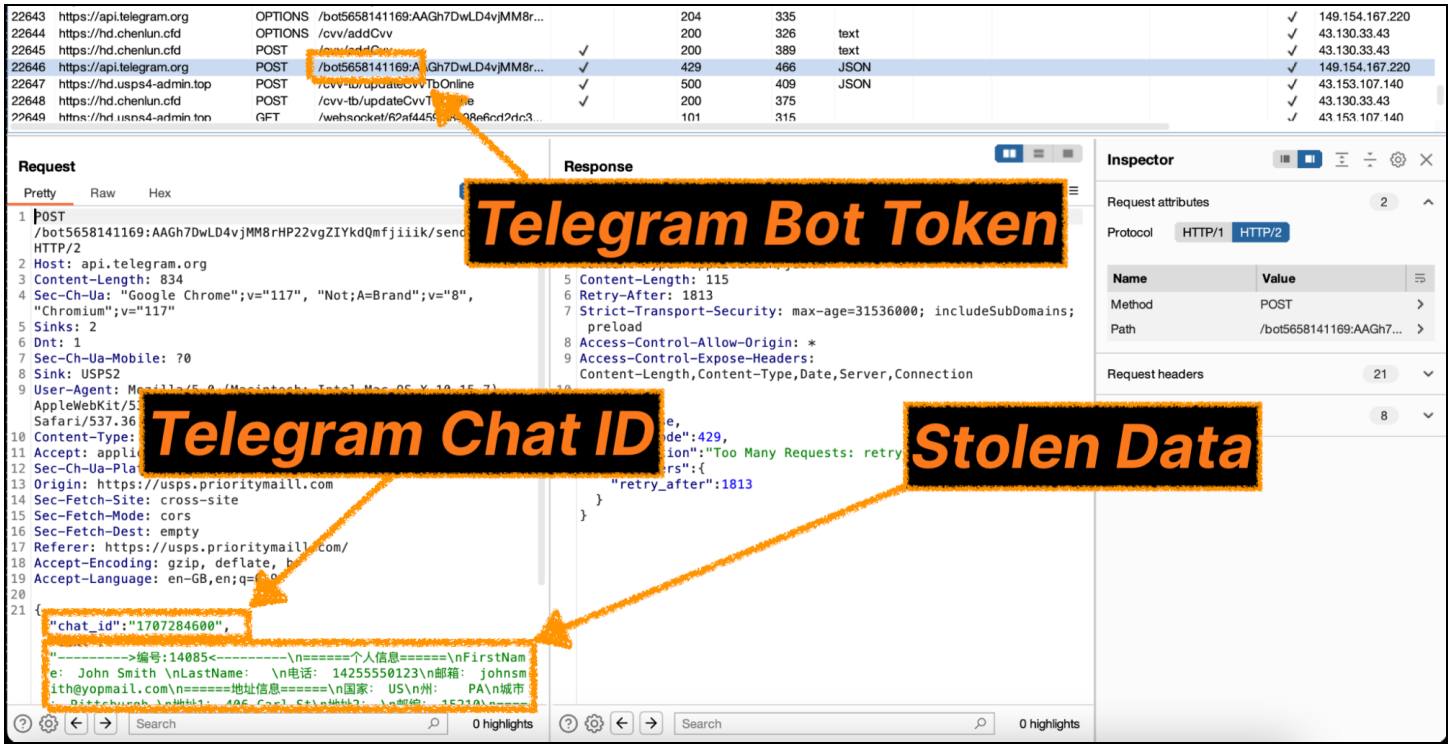


Figure 9: *Network captures revealed how the smishing campaign transmitted stolen data to a Telegram bot API (Source: Recorded Future)*

Scammers likely reuse their data-theft infrastructure to conduct subsequent scam campaigns, sometimes achieving truly global scale. Our analysis of stolen card data linked to scam websites distributed by the USPS-based smishing campaign revealed that the campaign had stolen at least 36,000 payment cards — and likely far more — issued from financial institutions in 95 countries. Over half of these payment cards originated from Australia, suggesting the campaign's infrastructure had previously been used for a major Australian scam campaign.

Once they have obtained victims' payment card data, scammers post the stolen payment cards for sale on dark web carding shops, where "end-user" fraudsters purchase the payment cards to conduct payment fraud. The China-based scam campaign resulted in at least 67,500 payment cards being posted for sale on 2 dark web carding shops; by our calculations, the operators of this campaign likely earned $500,000 in revenue from sales of these payment cards. On another carding shop, we attributed for-sale payment card databases containing over 30,000 stolen payment cards to merchant accounts at suspected scam websites from various scam campaigns.

Takeaways: Banks and consumers should consider "scammed" personal or financial data to be at high risk of compromise, even if subsequent fraud has yet to occur. Financial institutions can mitigate this risk by reissuing payment cards or raising their risk scores.

Dark Web Offerings Help Scammers Easily Apply Sophisticated Scam Tactics at Large Scales

Implementing these advanced methods may seem like a tall order, but third-party "fraud-as-a-service" offerings on dark web sources simplify the task. Some of these offerings are holistic, such as the phishing services promoted by @chenlun, the threat actor responsible for operating the USPS-based smishing campaign. In a detailed analysis, the researcher g0nxja identified smishing texts, phishing pages, and "dual working" domain dashboards used to access exfiltrated data as 3 primary elements of another Spanish "Xibanya" smishing/scam campaign operated by @chenlun. The presence of these elements across 2 campaigns operated by @chenlun indicates that the threat actor offers scammers a holistic, all-in-one service for disseminating, creating, operating, and securely retrieving stolen data from scam websites.

A variety of other specialized dark web services, tools, and step-by-step tutorials are also available to scammers looking to develop or outsource the operation of their scam campaigns, including:

- Design services for scam ad lures, websites, and landing pages (Figures 10 and 11)
- SMS spam/smishing services (Figure 12)
- Web traffic services for driving victims to scam websites (Figure 13)

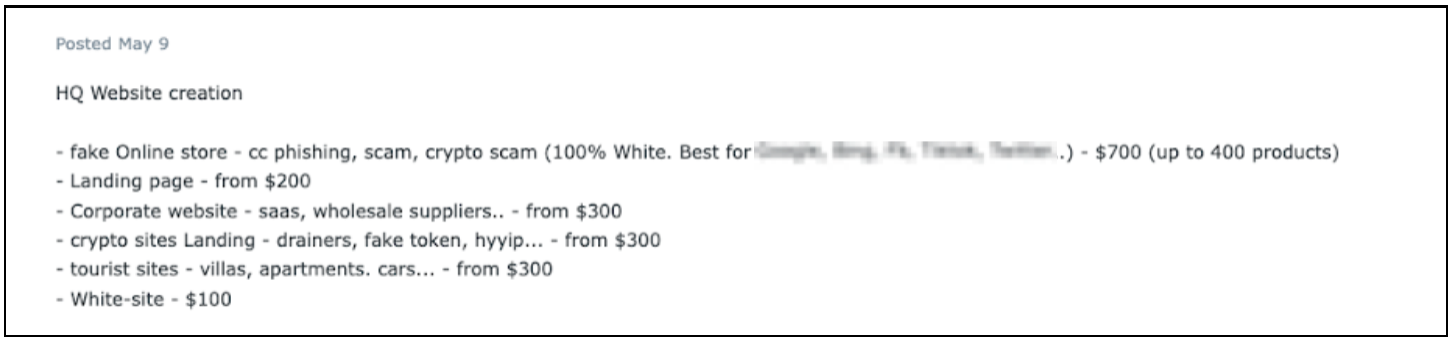


Figure 10: *A threat actor advertised a service that scam operators can use to create custom scam websites with online store functionality, landing pages, and more (Source: Top-tier dark web forum)*

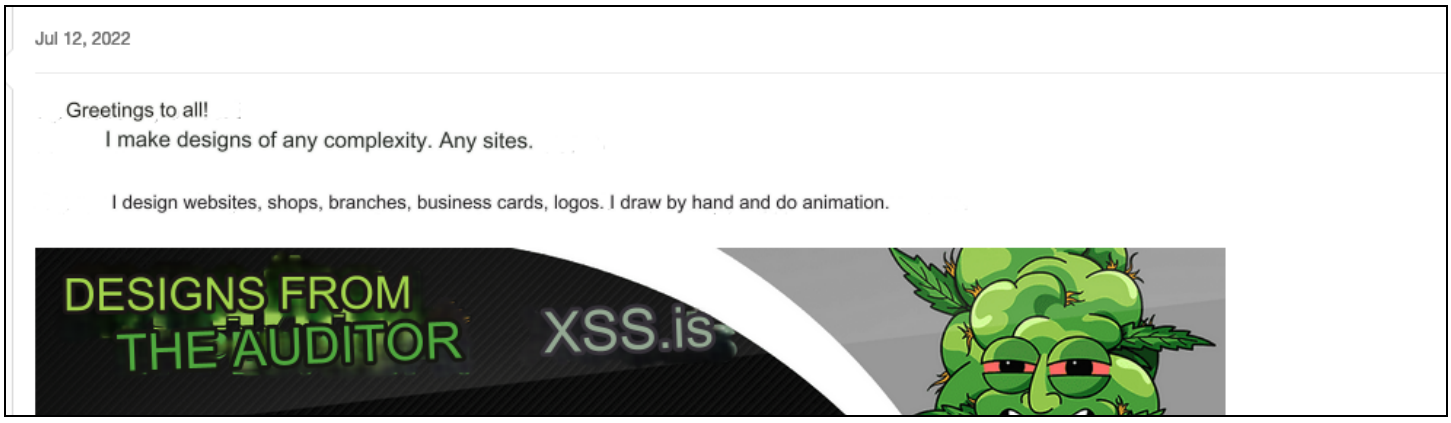


Figure 11: *Scammers can take advantage of a design service promoted by this threat actor to design scam websites, landing pages, and ad lures (Source: Top-tier dark web forum)*

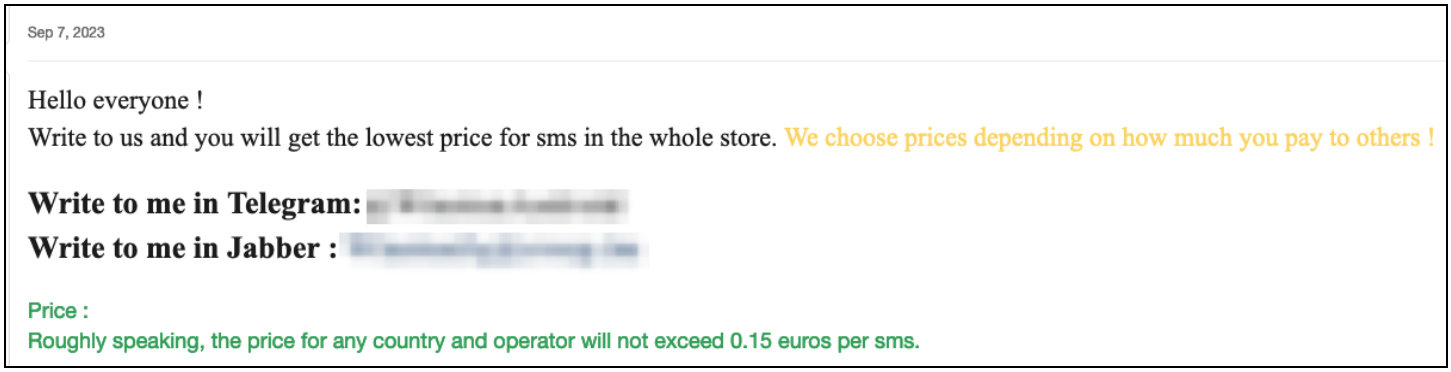


Figure 12: *A smishing service promoted by this threat actor allows threat actors to disseminate their scam websites via SMS text messages at scale (Source: Top-tier dark web forum)*

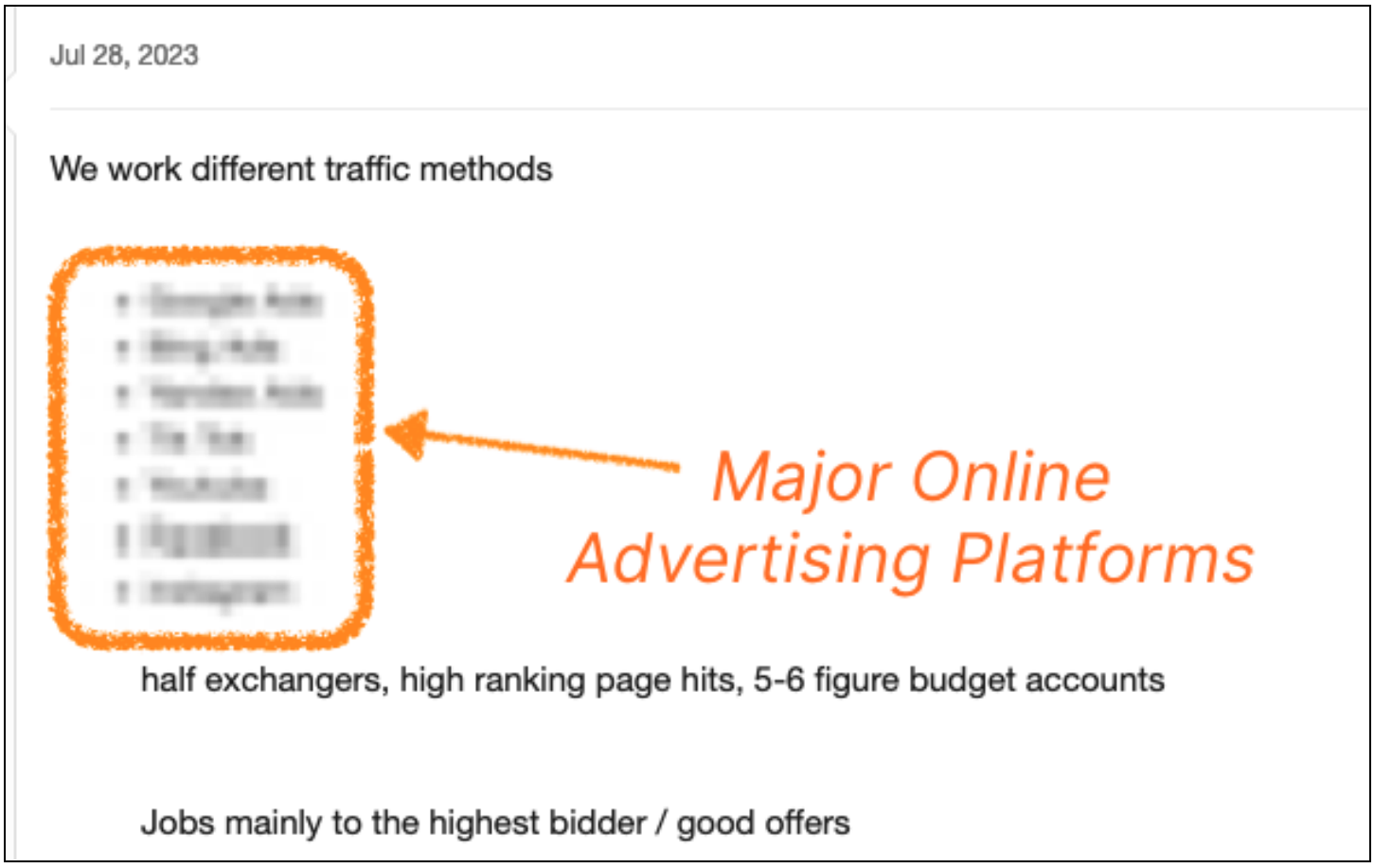


Figure 13: *A threat actor promoted a service that scammers can use to drive legitimate ad traffic to their scam websites (Source: Top-tier dark web forum)*

Takeaways: For scammers seeking to conduct advanced scam campaigns at scale, third-party dark web services lower barriers to entry and create opportunities to rapidly implement advanced solutions to disseminate scam websites, cash-out victims' payment cards and bank accounts, and steal victim data.

Scam Websites Exploit Consumer Psychology to Maximize Impact

At its heart, a scam is essentially a confidence game. To steal money from victims, the victims must first share sensitive financial or PII data with the scam website. For victims to trust scam websites enough to share sensitive information, the scam website must be credible. To design credible scam websites and ad lures, scammers must display a shrewd understanding of consumer psychology. This exploitation of psychology to trick victims is a vital element of social engineering.

Scam operators use various tactics to entice victims into falling for scams. According to January 2023 research published by the British Journal of Criminology, fraudsters employ urgency and time pressure, authority, flattery, emotional appeals, and other language-based techniques to compel victims to cooperate. Our analysis of various scam campaigns corroborates these findings. In many cases, scam websites make use of bogus limited-time offers, discounts, and free trial offers to increase victims' sense of urgency, compelling them to make a purchase or submit personal information before they have verified the legitimacy of the website.

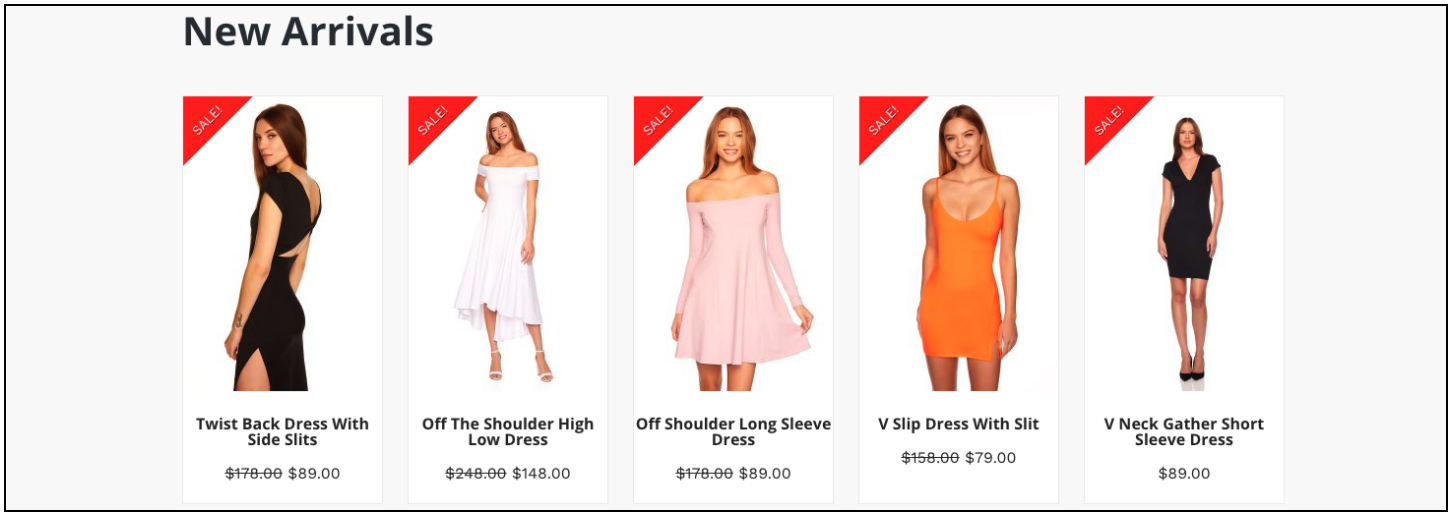


Figure 14: *This likely scam website uses discount offers to increase users' sense of urgency (Source: Recorded Future)*

Similarly, scammers use sales funnels to increase victims' conversion rates for their scams, likely emulating a marketing paradigm referred to as "the buyer's journey". With this approach, scam ads and websites are designed to encourage victims to act incrementally. For example, text messages from the smishing campaign included links to landing pages, which then redirected victims to the scam website home page. On the scam home page, victims were instructed to submit their personal and financial data piecemeal on sequential forms in order to update their shipping information for a bogus delivery. Breaking down a scam website's attack chain into smaller steps may facilitate the scam's ultimate success.

In some cases, scam websites appear to use sophisticated methods to discourage victims from reporting or successfully disputing scam charges to receive chargebacks. The subscription scam

campaign we identified was reported to use social media ads to redirect victims to payment forms rather than the scam website's home page, where they were promised a "prize giveaway" after they paid a trial fee. However, if accessed via search engine referral, these same scam websites clearly displayed their refund and payment logic, likely to complicate fraud investigations or discourage victims from reporting the subsequent scam subscription charges. The same campaign also purported to sell services rather than goods, which may have been intended to complicate fraud disputes.

Scammers also use social media and messenger services to amplify the impact of their scam websites. In these cases, the scam operators are likely aware that potential victims may research businesses on the web before making a purchase with them. For the China-based scam campaign, the scam operators created Facebook business profiles for 20% of their scam domains in a likely effort to increase their online scam shops' credibility. These pages notably recycled the text used on their corresponding scam websites' "About Us" pages — likely another demonstration of scammers' preference for quantity over quality.

Finally, scam website operators use evolving typosquatting techniques to fool victims into trusting their fraudulent domains. The USPS-based smishing campaign and its linked network of scam websites used "downshifted" domains that incorporated text from top-level domains into their typosquatted second-level domains (for example, in the domain *com-ny[.]store*). This technique likely reduced the probability that victims would detect the fraudulent domain while also allowing the scam operator to target multiple brands for impersonation using different subdomains.

Notably, the same threat actor has already used the same technique to register fraudulent domains modeled after the official *[.]gov* domain of the US Internal Revenue Service (IRS), likely in anticipation of next year's tax season (for example, *irs[.]gov[.]payment-tax[.]com*). As the wheel turns, so do the scams.

Takeaway: Increasing customer awareness is crucial to protecting customers from scams. Educate customers regarding the specifics of the threat posed by scam websites, how they operate, what indicators to be aware of, and what techniques scammers have employed in recent scam campaigns.

Mitigations

Identification, Analysis, and Prevention

- Solicit scam website leads from your customers to identify potential scam websites. Provide leads to your internal cyber threat intelligence (CTI) teams or external CTI provider for analysis.
- Analyze confirmed scam websites' domain registration information, network infrastructure, and website configuration and design. Extrapolate these elements in an expanded search to identify related scam websites. Scam website campaigns depend on scale for success — where there's one, there are likely to be more.

- Flag merchant accounts associated with numerous reported scam transactions as fraudulent. Research common elements between identified scam merchant accounts — for example, acquirer BINs and MCCs — to surface blocks of related scam merchant accounts. Raise fraud risk scores for all transactions conducted with identified scam merchant accounts.
- Review fraud intelligence reporting to stay abreast of trending scam threats to your customers and your organization.
- Educate customers regarding the specific threat posed by scam websites, what indicators to be aware of, and specific techniques employed by scammers. Train customers to recognize and avoid potential scam websites.

Customer Awareness and Education

- Be cautious of online advertisements, especially on search engines and social media. Use ad blockers.
- Report scams to your payment card issuer and/or the Better Business Bureau (BBB), and dispute losses to attempt to recover your funds through chargebacks. Report scams to law enforcement.
- Only provide financial and personal information to secure, trusted websites.
- Verify the legitimacy of e-commerce websites and their payment subdomains before making purchases. Check the website's URL, ensure that it uses HTTPS, and compare it to the official website's URL.
- Research companies before you make purchases from them. Review complaints on the BBB's official website, ask trusted sources, or perform a web search to understand other consumers' experiences with the company.
- Understand the terms and conditions for your purchases, and be aware that honest businesses do not hide these terms from customers. Do not continue with a purchase if the terms and conditions differ from your understanding of the offer. Be wary of pre-checked boxes that may give your consent to sign up for expensive subscriptions.
- Understand how to cancel subscriptions or terminate paid memberships. Free trials may have a time limit before automatically initiating subscriptions; ensure that you understand these deadlines.
- Be wary of unsolicited communications. Scam operators may use phishing or smishing lures to disseminate their scam websites.
- Research common scams and phishing techniques, and remain vigilant when interacting with online social media content.

Outlook

The threat posed by scam websites, particularly online shopping scams, is likely to continue to grow. Although this threat may be more salient at certain times of the year, businesses and consumers should never lower their guard. While consumers may be more vulnerable to scam campaigns on Black Friday, the underlying nature of the scam threat is largely unchanging. Similarly, although the specifics of how scammers operate may evolve over time, the underlying rationale for their tactics is likely to remain constant — as are the key takeaways for consumers and businesses looking to protect themselves.

Given the tendency of scam websites to exploit human nature and reuse infrastructure to achieve scale, customer education and campaign analysis will likely continue to be the most enduring, viable mitigation strategies for reducing the risk posed by scam websites.

Moreover, various sources indicate that the advent of generative AI will likely amplify the threat posed by scam websites by lowering barriers to entry for scam operators, whom AI will continue to empower to swiftly generate content for scam websites and scam ad lures. Previously, Insikt Group's report "I, Chatbot" indicated that threat actors have developed methods for employing ChatGPT to support social engineering, phishing, malvertising, and money-making schemes, all of which can magnify the impact of scam websites. Likewise, a 2023 biannual threats report authored by Visa Payment Fraud Disruption and an article by the American Banking Association both indicate that AI will raise the threat potential of phishing and scam schemes.

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.