Scams at Scale: Unmasking crypto fraud and social engineering on the modern web

From legitimate-looking cryptocurrency investment portals to fake celebrity giveaways, scammers are building sophisticated campaigns that exploit users' trust across the web to deprive them of their life savings. In this article, we unpack how some of these campaigns operate at scale and how researchers can systematically detect, track, and stop them.

By Abisheka Pitumpe, Muhammad Muzammil, Xigao Li, Nick Nikiforakis, and Amir Rahmati

DOI: 10.1145/3744694

"Hey, I think you have the wrong number," Maria typed back to the unfamiliar contact. Three months later, she transferred her life savings to a cryptocurrency investment scheme that never existed.

This story is becoming disturbingly common. What begins as a random text message or social media comment can evolve into a long-form confidence game with devastating financial consequences. Social engineering has shifted from clickbait phishing links to sophisticated manipulation campaigns that unfold over weeks or even months.

Today's digital scammers are relationship architects. They don't just trick; they befriend. They cultivate trust, sometimes even romance. They "fatten" their victims methodically, nurturing connections until the moment is right for financial exploitation. The emotional investment made before any money changes hands creates a powerful cognitive blind spot—one that traditional security education often fails to address.

The rise of blockchain technology and the near-universal accessibility of the internet have given rise to a new kind of adversary: one that blends automation, psychological manipulation, and financial fraud. Operating at a massive scale, these attackers resemble global criminal syndicates more than lone hackers. With platforms like YouTube and X (formerly Twitter) connecting billions of users, scammers gain unlimited opportunities to exploit trust and shape perception. With cryptocurrency enabling untraceable, irreversible transactions, the perfect storm for modern scams has arrived.

The FBI reported that there were more than $5.6 billion in losses in 2023 caused by cryptocurrency scams alone [1]. This number is a testament to the many victims who fall for these scams every day and emphasizes how important it is to investigate these attacks. Through the lens of research systems developed by the Ethos and PragSec labs at Stony Brook University, we explore the scale and sophistication of these scams and the infrastructures that support them.

Image by PK Designs/ Shutterstock.com

UNMASKING GIVEAWAY SCAMS

While investment scams rely on the professional design of a website to lure people, social media giveaway scams leverage virality and the use of recognizable figures. The scams use pictures and names of crypto influencers and celebrities, urging followers to send coins to receive double. The scam is simple but effective, especially when it rides the momentum of trending events.

By tracing 2,266 fraudulent wallet addresses in major blockchains, we identified between $24.9 million and $69.9 million in losses. In just six months, CryptoScamTracker flagged more than 10,000 scam websites [2]. These figures come from direct blockchain analysis, not victim reports, offering one of the most precise financial assessments of web-scale fraud to date.

Interestingly, attackers often reused domains, shared infrastructure, and re-victimized users with "recovery scams" that offered to help retrieve lost funds for a fee.

CATCHING INVESTMENT SCAMS IN REAL TIME

Crimson[1] is a system to longitudinally detect cryptocurrency investment scam websites in the wild as soon as they are created [3]. The design of Crimson is modular; it leverages certificate transparency (CT) logs to capture every domain that receives a transport layer security (TLS) certificate and then filters these domains by identifying suspicious keywords. The

1 https://github.com/pragseclab/Crimson

corresponding web pages are analyzed using screenshots, object character recognition (OCR), and HTML code, further narrowing the list. Using the large language models Llama3 and GPT-4, we classified each website as either a scam or legitimate. Additionally, Crimson includes a module for automatically signing in to scam websites and extracting cryptocurrency wallet addresses provided by scammers. Over time, Crimson monitors these websites, tracking behaviors such as shutdowns, reactivations, and changes in hosting providers.

Between January and September 2024, Crimson detected 43,000-plus scam websites, spanning 38,000 unique second-level domains, and 19,000 IP addresses. Our analysis revealed that many of these websites were hosted on a small number of IP addresses, with 52% of them residing on only 10% of all IPs. Furthermore, approximately 40% of scam websites shared similar design features, forming 4,300 clusters. Scam websites include modern interfaces, fake reviews, counterfeit certificates, and fake notifications such as "Dustin from Anaheim just earned $41,851.25 minutes ago."

Interestingly, these websites also reused identical phone numbers and wallet addresses, indicating coordinated scam operations. Our monitoring also revealed the persistence of these websites, with around 23,000 (47%) remaining active at the end of the study period. Many scam sites became temporarily inactive, only to reactivate later, often under a different hosting provider. The financial losses from these scams were substantial, with just 6.7% of websites responsible for $2.7 million in losses. Overall, the estimated total financial loss exceeded $100 million, with an average victim payment of approximately $3,700. We also found that many popular block-lists, such as Google Safe Browsing, failed to identify more than 98% of scam websites, reiterating the lack of proper detection and prevention mechanisms for such scams.

YOUTUBE AS A LAUNCHPAD FOR FRAUD

YouTube comment sections have become a fertile ground for social engineering attacks. Scammers use bots to flood high-profile videos with deceptive comments, often impersonating creators and advertising investment or prize opportunities via WhatsApp and Telegram.

We monitored 20 YouTube channels for six months, capturing 8.8 million comments [4]. Using a series of filters—textual (keywords and obfuscation), visual (profile imagehashing), and temporal (comment frequency and sequencing)—we identified more than 206,000 scam comments linked to 10,000 unique accounts. Scammers used visually similar Unicode characters to evade detection by YouTube's spam filters. Some created fake dialogues between multiple accounts to create the illusion of authenticity. Despite YouTube's takedown efforts, 70% of these accounts remained active at the end of the study period.

We interacted directly with 50 scammers to understand their tactics and payment preferences. Almost all requested cryptocurrency payments, and many used U.S.-based phone numbers while operating from other time zones. These conversations revealed highly scripted social engineering designed to build trust gradually, often over several days.

BLOCKCHAIN NAMING SERVICES

As the Web3 ecosystem continues to expand, blockchain-based naming services (BNSs), such as the Ethereum Name Service (ENS), have been developed to map human-readable domain names to cryptocurrency addresses similar to the traditional domain name system (DNS). This functionality simplifies transactions by eliminating the need for users to memorize long and complex wallet addresses and helps mitigate common attacks such as address poisoning [5–7]. However, these naming services are not immune to exploitation. Traditional DNS attacks, such as cybersquatting and domain dropcatching, can also affect BNSs, leading to significant financial losses for unsuspecting users.

Today's attackers weaponize trust at a global scale. Instead of exploiting software vulnerabilities, they exploit human vulnerabilities

We conducted two large-scale measurement studies, focusing on understanding and analyzing dropcatching attacks and typosquatting in BNSs [8, 9]. To perform these studies, we curated and open-sourced the largest public dataset of BNS domains to date, comprising more than 5 million domains across ENS, unstoppable domains, and ADA handles.[2,3]

Dropcatching occurs when domain owners fail to renew their ENS domain before it expires, making the domain available for re-registration by others. Typosquatting in BNSs occurs when attackers register typographically similar variations of popular domain names, waiting for users to make a mistake when typing the domain, inadvertently and irreversibly sending funds to the attacker's address. For example, a user who intends to send funds to vitalik.eth, owned by Ethereum founder Vitalik Buterin, might accidentally send funds to vitalikk.eth instead, which could be registered to an attacker.

Our study revealed that typosquatting is a widespread issue in BNSs, with 37% of popular ENS domains being targeted by at least one typosquatting domain [9]. In addition, we identified thousands of transactions sent to the addresses of typosquatting domains. We also observed a consistent increase in the registration of typosquatting domains over time. Interestingly, squatters were particularly interested in domains linked to high-profile individuals and cryptocurrency influencers on social media

2 https://github.com/pragseclab/typosquatting3.0
3 https://github.com/pragseclab/ens-dropcatching

platforms (e.g., vitalik.eth or mariogotze.eth). The analysis of transactions directed to typosquatting domains revealed that attackers were able to misdirect significant funds into their wallets, with the average transaction being $1,790.

In parallel with the study on typosquatting, we also conducted a large-scale investigation into ENS domain dropcatching [8]. Attackers can exploit this opportunity to re-register expired domains and update the associated cryptocurrency wallet addresses to their own. As a result, any funds sent to the expired domain after its re-registration will be misdirected to the attacker's wallet instead of the intended recipient.

Our findings revealed that more than 241,000 ENS domains were re-registered after expiration. We found that domains previously associated with higher incomes were more likely to be targeted by attackers. In total, our study identified more than 2,600 transactions that were misdirected to new owners of expired domains, with an average of $4,700 per transaction.

Notably, our study highlighted a significant gap in popular digital wallet protections, both custodial (e.g., Coinbase) and non-custodial (e.g., MetaMask). In both the typosquatting and dropcatching contexts, these wallets failed to display any warnings to users before they mistakenly sent funds to malicious typosquatting domains or re-registered ENS domains.

CONCLUSION

Across our investigations into giveaway scams, investment frauds, blockchain naming service abuse, and YouTube comment scams, a consistent and unsettling picture emerges: Today's attackers weaponize trust at a global scale. Instead of exploiting software vulnerabilities, they exploit human vulnerabilities—leveraging automation, social influence, and the infrastructure of the modern web to deceive and defraud. The studies we conducted demonstrate that scalable, real-time detection is not only possible but essential. Tools like CryptoScamTracker and Crimson show that CT logs can be repurposed into a global early-warning system for scam websites. Our studies of blockchain-based naming systems highlight how traditional cybercrime techniques, like typosquatting and domain hijacking, have seamlessly transitioned into the Web3 era. Even spaces that feel inherently human, like comment sections on YouTube, are being colonized by automated, persistent fraud campaigns.

What begins as a random text message or social media comment can evolve into a long-form confidence game with devastating financial consequences

If there is a single takeaway, it is that cybersecurity must now address the socio-technical layer—the messy, human-facing interface where emotion, perception, and technology collide. Combating these new threats will require collaboration between platform providers, security researchers, blockchain developers, and policymakers. It will require building systems that are not only secure by design but also resilient against manipulation. And above all, it will require recognizing that trust—the very currency of the digital world—has become one of its greatest attack surfaces. The future of cybersecurity is a future of defending not just systems, but users themselves. Our research represents an early step toward that broader, necessary mission.

References

[1] Federal Bureau of Investigation. 2023 Cryptocurrency Fraud Report released. Sept. 10, 2024; https://www.fbi.gov/news/stories/2023-cryptocurrency-fraud-report-released

[2] Li, X., Yepuri, A., and Nikiforakis, N. Double and nothing: Understanding and detecting cryptocurrency giveaway scams. In *Proceedings of the Network and Distributed System Security Symposium* (NDSS). 2023.

[3] Muzammil, M. et al. The poorest man in Babylon: A longitudinal study of cryptocurrency investment scams. In *Proceedings of the ACM on Web Conference 2025* (WWW '25). ACM, NY, 2025, 1034–1045.

[4] Li,X. , Rahmati, A., and Nikiforakis, N. Like, comment, get scammed: Characterizing comment scams on media platforms. In *Network and Distributed System Security Symposium* (NDSS). 2024.

[5] Guan, S. and Li, K. Characterizing ethereum address poisoning attack. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security* (CCS '24). ACM, NY, 2024, 986–1000.

[6] He, B. et al. Txphishscope: Towards detecting and understanding transaction-based phishing on Ethereum. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS '23). ACM, NY, 2023, 120–134.

[7] Tsuchiya, T. et al. Blockchain address poisoning. *arXiv:2501.16681v1* [cs.CR].2025.

[8] Muzammil, M. et al. Panning for gold.eth: Understanding and analyzing ENS domain dropcatching. In *Proceedings of the Internet Measurement Conference* (IMC). 2024.

[9] Muzammil, M. et al. Typosquatting 3.0: Characterizing squatting in blockchain naming systems. In *Proceedings of the Symposium on Electronic Crime Research* (eCrime). 2024.

Biographies

Abisheka Pitumpe is a Ph.D. student in the Department of Computer Science at Stony Brook University. Her research Interest is in web security. Her work focuses on building automatic systems that can detect and measure internet scams at scale.

Muhammad Muzammil is a Ph.D. candidate in computer science at Stony Brook University, where his research focuses on internet measurements, privacy, and security. His work uncovers malicious activities and vulnerabilities in Web3 ecosystems.

Xigao Li is a research scientist at Meta Platforms. Inc. He earned his Ph.D. in computer science from Stony Brook University in 2023. His research interests are primarily detecting malicious web activities via automation.

Nick Nikiforakis (Ph.D. '13) is an associate professor in the Department of Computer Science at Stony Brook University. He leads the PragSec Lab, where his students conduct research in cybersecurity, with a focus on web and network security. He is the author of more than 90 peer-reviewed academic publications, and his work is often discussed in the popular press. He is the recipient of the National Science Foundation CAREER award (2020), the Office of Naval Research Young Investigator Award (2020), as well as a range of other security-related and privacy-related awards by federal funding agencies. Next to multiple best-paper awards, the National Security Agency awarded him the "Best Scientific Cybersecurity Paper" award for his research on certificate transparency abuse in 2023.

Amir Rahmati is an assistant professor of computer science and director of the Ethos Security & Privacy lab at Stony Brook University. He earned his Ph.D. in computer science and engineering from the University of Michigan in 2017. His research focuses on understanding emerging security and privacy threats in computer systems and building practical solutions to tackle them. His work has resulted in tens of publications and patents, as well as thousands of citations. Rahmati's work is supported by the Air Force Office of Scientific Research (AFOSR), Office of Naval Research (ONR), Samsung, Meta, NVIDIA, and IBM. His research has received multiple awards and frequent attention from media outlets, including *MIT Technology Review, The Washington Post,* and Bloomberg. Artifacts from his work on the security of autonomous driving systems are part of the permanent collection of the London Science Museum. He is a senior member of the National Academy of Inventors (NAI) and IEEE.

1528-4972/25/06 $15.00