

Internet Fraud

Clarrissa Darden

Cyber Criminology Foundation

Arif Akgul, Ph.D.

October 27, 2025

The rise of digital technology has reshaped every part of modern life from how we communicate, work, shop, and even think. But it's also created countless new opportunities for crime. Cybercrime has evolved from isolated hacking incidents into complex global systems of fraud, surveillance, and manipulation. These crimes don't just target banks or governments anymore; they affect ordinary people scrolling on their phones or sharing personal data online.

This analysis uses ten recent news articles from The New York Times and Taranaki Daily News to explore current cybercrime trends between 2023 and 2025. While exploring current cybercrime trends five major themes emerged: (1) the rise of online scams and social engineering, (2) the struggle between digital freedom and surveillance, (3) misinformation as a political weapon, (4) the globalization of cybercrime and its enforcement challenges, and (5) the erosion of trust in a digital world.

The rise of online scams and social engineering

The most visible and personal type of cybercrime is online fraud. The rise of online scams and social engineering thrives because it preys on trust, confusion, and the human tendency to act fast when scared. In *"I've Written About Loads of Scams. This One Almost Got Me,"* journalist Michael Wilson (2025) describes how professional scammers impersonated Chase Bank representatives and nearly tricked him into sending \$2,100 via Zelle. His experience shows how criminals use fake authority and urgency to control victims' reactions, turning even cautious people into easy targets.

Similarly, Steven Kurutz's *"Welcome to Scam World"* (2024) and *"You're Surrounded by Scammers"* (2024) highlight how digital fraud has become an inescapable part of daily life. People face scams through text messages, fake job offers, and deepfake videos all blending into a digital environment where it's increasingly hard to tell what's real. Kurutz (2024) explains that the constant exposure to these scams leaves people "in a heightened state of vigilance," showing how cybercrime doesn't just steal money it erodes trust in technology itself.

This theme also appears in *"Internet Fraud Under the Spotlight at Forum"* (Girling-Butcher, 2025), where community groups in New Zealand host events to educate seniors about online fraud. This local response emphasizes that preventing scams isn't only a technical issue, it's also about public awareness. The emotional manipulation seen in scams from fake customer service calls to cryptocurrency hoaxes demonstrates that cybercriminals succeed not because of advanced coding, but because they understand human behavior.

The struggle between digital freedom and surveillance

While scammers exploit individuals, governments and corporations have also expanded their ability to monitor online activity, but there is a struggle between digital freedom and surveillance. In *"National ID for Online Is Proposed by China,"* Tobin and Liu (2024) report that Chinese regulators are developing a centralized "internet ID" that would allow the government to track citizens online behavior. Though the plan is marketed as a privacy safeguard, critics warn that it could intensify state surveillance and make anonymity impossible.

This tension between digital safety and freedom is also seen in “*Taiwan, on China’s Doorstep, Is Dealing with TikTok Its Own Way*” (Tobin & Chien, 2024). Taiwan faces a constant flood of pro-China disinformation on TikTok but resists a full ban to preserve free speech. The country’s approach shows how democracies must balance security against censorship. Instead of banning platforms, Taiwan invests in fact checking networks and digital literacy programs.

These examples reveal a paradox: both authoritarian and democratic governments justify surveillance in the name of security. Yet, as Tobin and Liu (2024) suggest, systems designed to “protect privacy” often end up concentrating power in ways that undermine it. The growing normalization of digital monitoring whether by governments or corporations, signals a shift toward a world where privacy is no longer assumed, but negotiated.

Misinformation as a political weapon

Cybercrime isn’t always about money; it’s also about influence. Information manipulation has become one of the most dangerous digital crimes because it targets democracy itself. “*Voter Fraud, A Few Go to Jail, As Others Don’t*” (Wines, 2023) examines how exaggerated claims of voter fraud have fueled political division in the United States. While actual fraud cases are rare, misinformation about them spreads rapidly online, shaping public opinion and policy.

This weaponization of digital misinformation was also central to “*Jan. 6 Panel Outlines Trump’s Bid to Coerce Justice Dept. Officials*” (Broadwater & Benner, 2023). The article details how former President Trump and his allies pressured officials to support false claims of election corruption. These actions relied heavily on digital platforms to amplify conspiracy theories, proving how misinformation can merge with political power to undermine institutions.

The pattern repeats globally. In Taiwan, fake videos and manipulated content on TikTok have been traced back to pro-China groups (Tobin & Chien, 2024). Disinformation is now a transnational crime tool used to destabilize societies from within. Unlike traditional cyberattacks that target hardware, misinformation attacks human psychology, exploiting biases and emotions to reshape reality.

The globalization of cybercrime and its enforcement challenges

Cybercrime today is borderless, moving faster than international law can respond. In “*On Lawless Asia Border, Outposts of Global Scam Thrive at Online Fraud*” (Beech, 2025), massive scam compounds in Myanmar and Thailand are run by transnational criminal groups using forced labor. These operations combine human trafficking, financial fraud, and digital deception into a single enterprise worth billions. Victims are not only the people losing money online, but also the trafficked workers forced to commit crimes.

This global dimension also connects to domestic experiences. As Steven Kurutz (2024) notes, scammers in “Scam World” can target millions with a few clicks using spoofed numbers and automated bots. The internet’s global scale gives cybercriminals the same advantages as multinational corporations cheap labor, anonymity, and cross-border reach.

International cooperation is improving, but slowly. The *Taranaki Daily News* article (Girling-Butcher, 2025) shows how local banks educate the public about online safety, but such community efforts are no match for international crime syndicates. Without stronger coordination between governments, cybercrime will continue to thrive in the gaps between laws and borders.

The erosion of trust in a digital world

A common thread through all ten sources is the erosion of public trust. Whether it's scams, misinformation, or surveillance, every case shows how people are losing confidence in digital systems. In "*Welcome to Scam World*," Kurutz (2024) writes that "the legitimate world looks so much like a scam that it's easier to make a scam look legitimate." That quote perfectly summarizes today's cyber landscape, the lines between authenticity and deception have blurred.

From Wilson's near-miss with the Zelle scam to Beech's accounts of human trafficking for online fraud, people are living in a world where even everyday interactions emails, bank calls, social media feel unsafe. This constant uncertainty creates anxiety and skepticism that extends beyond technology, influencing how people view government, media, and even each other.

Conclusion

Across all ten articles, cybercrime emerges as more than a technical issue it's a social crisis that affects trust, privacy, and democracy. The themes of fraud, surveillance, misinformation, and globalization reveal a world where crime has adapted to the pace of technology faster than laws or ethics can. Scammers exploit fear and convenience; governments exploit data and security; and everyday people are left to navigate the internet that feels increasingly unsafe.

The future of cybersecurity will depend on balancing innovation with accountability. International cooperation, digital education, and stronger privacy protections are essential to rebuild trust online. As these stories show, cybercrime doesn't just happen in dark corners of the internet, it's woven into the systems we use every day.

AI Tool Usage Declaration

This paper was developed with assistance from ChatGPT (GPT-5, OpenAI) for theme organization, and APA formatting. All analysis, interpretations, and source integration were performed by Clarrissa Darden. The AI was used ethically in accordance with academic integrity guidelines.

References

Beech, H. (2025, March 2). *On lawless Asia border, outposts of global scam thrive at online fraud. The New York Times.*

Broadwater, L., & Benner, K. (2023, June 23). *Jan. 6 panel outlines Trump's bid to coerce Justice Dept. officials. The New York Times.*

Girling-Butcher, L. (2025, August 18). *Internet fraud under the spotlight at forum. Taranaki Daily News.*

Kurutz, S. (2024, April 21). *Welcome to scam world. The New York Times.*

Kurutz, S. (2024, April 21). *You're surrounded by scammers. The New York Times.*

Tobin, M., & Chien, A. (2024, May 16). *Taiwan, on China's doorstep, is dealing with TikTok its own way. The New York Times.*

Tobin, M., & Liu, J. (2024, August 1). *National ID for online is proposed by China. The New York Times.*

Wilson, M. (2025, September 18). *I've written about loads of scams. This one almost got me. The New York Times*

Wines, M. (2023, September 8). *Voter fraud, a few go to jail, as others don't. The New York Times.*