“Many drawn into yami-baito, becoming both “victims and offenders,” are students, school dropouts, or precariously employed young people facing economic hardship or social isolation

Overcoming the anonymity–trust dilemma

Youth-centred solutions informed by the case of Japan's yami-baito

by **Rin Tsuboyama**

A crime that shattered illusions

In May 2023, a luxury watch store in Ginza – one of Tokyo's most prestigious districts – was stormed by three masked youths wielding hammers. The brazen daylight raid was so surreal that some passersby mistook it for a movie shoot. Yet it was a real crime.

> **"Within an hour, police arrested four suspects, all aged 16-19, brought together via an anonymous recruitment post on social media."**

They were pawns in what is known in Japan as yami-baito – literally "dark part-time jobs"– a rapidly proliferating form of criminal recruitment advertised on social networking sites or encrypted messaging apps. In this case, teenagers with no prior criminal records had been lured through encrypted chats into acting as perpetrators under the pretext of "easy money." The episode vividly shows how the anonymity of cyberspace can draw Japanese youth into severe crimes in the physical world.

Inside the shadow economy of yami-baito

The Ginza robbery is only the tip of the iceberg. In recent years, intensified crackdowns on organized crime have weakened Japan's traditional yakuza syndicates, paving the way for highly fluid and anonymous criminal groups known as tokuryū. These loosely organized networks recruit online via Twitter, Instagram, Telegram, or job-search apps. According to the National Police Agency's 2024 report, of the 2,373 people arrested in 2023 for acting as perpetrators in special fraud or robberies, about 42% became involved through yami-baito (dark part-time jobs) ads on social media. Over 30% joined through referrals from acquaintances, suggesting peer-to-peer recruitment. Tasks range from transporting illicit funds to violent home-invasion robberies – well beyond "harmless mischief."

Many drawn into yami-baito, becoming both "victims and offenders," are students, school dropouts, or precariously employed young people facing economic hardship or social isolation. Recruiters exploit anonymity, posing as providers of "high-paying jobs" or "exclusive group member-

ships." Backing out can be perilous: in many cases, attempts to withdraw have triggered threats against families. Police have taken protective measures in over 125 such cases – underscoring the real danger.

The double-edged sword of online anonymity

The spread of yami-baito in Japan highlights an "anonymity–trust dilemma" in the digital age. Online anonymity and encrypted communication protect privacy and free expression, enabling young people to seek advice or explore identity without fear of stigma. Many constructive activities – such as whistleblowing and identity exploration – depend on it. Yet the same anonymity makes identifying perpetrators difficult and erodes trust online.

> **"Criminal recruiters operate under pseudonyms and disappearing messages, evading detection while approaching youth who cannot easily judge trustworthiness."**

The Australian eSafety Commissioner, for example, calls this a "double-edged" quality, urging balance to curb abuse without undermining legitimate benefits. I agree, but the key question is: what concrete measures can achieve such balance? Below are proposals to preserve the constructive aspects of online anonymity while ensuring safety and trust.

Charting a path out of the anonymity–trust dilemma

Tech and design for safer platforms

A priority is strengthening technical safety on platforms used by young people – from social networking services (SNSs) to job-matching sites. These should proactively detect and block illegal recruitment. AI-based moderation could flag suspicious job offers ("easy money," "high income for little effort") or links to encrypted apps, subjecting them to review and removal. Risky acts, like posting recruitment ads anonymously, could require extra verification, such as age or identity checks via zero-knowledge proofs. Pop-up warnings – "This may be an illegal recruitment attempt such as yami-baito" – and links to counseling services could appear when users exchange contact info or move off-platform.

Educating and protecting the next generation

Equally crucial is equipping youth with knowledge. Schools, families, communities, and police must collaborate on awareness campaigns explaining yami-baito and online fraud. This could include formal instruction in middle and high schools or shareable content – videos, comics – on social media. Support channels such as anonymous, free hotlines and chatbots can offer early intervention. It must be clear that even if individuals are already involved, seeking help will bring protection, not condemnation.

Uniting forces across borders

Combating yami-baito and similar crimes may exceed any single country's capacity. For example, numerous youths, including Japanese, have been rescued from factories in Myanmar where they were forced into telephone fraud – a cross-border hybrid of online and physical exploitation. There is also the risk of Japan's crime patterns being "exported" abroad. Addressing this requires collaboration between the public and private sectors and across borders. Law enforcement, tech companies, and organizations like the International Criminal Police Organization (INTERPOL) should create joint platforms for intelligence sharing, reporting recruitment tactics, and tracking dark web trends. Data from Japanese police – such as keywords used in recruitment or targeted age groups – could aid overseas monitoring.

Conclusion: shedding light on the dark side of the internet

The yami-baito phenomenon in Japan is a warning to the global community. It shows how the benefits of an open Internet can become a breeding ground for crime, posing urgent questions about trust and privacy.

> **"Yet solutions exist: combining cryptographic verification, decentralized trust systems, user-centered education, and safety-by-design principles can enhance safety without sacrificing privacy."**

The anonymity–trust dilemma will not be solved overnight, but with coordinated technological, educational, and institutional efforts, we can curb crimes exploiting anonymity while preserving its freedoms – moving toward a cyber environment illuminated by its benefits rather than obscured by its abuses.

About the Author

Rin Tsuboyama is an MSc Sociology student at the University of Oxford and a Visiting Research Fellow at Japan's Council for Public Policy. He also serves as a Researcher at the Institute of Geoeconomics and as Japan's representative for the economic and demographic imbalances track at the Y7 Summit France 2026. He holds a BA in Sociology from the University of Tokyo. His research focuses on the sociology of trust, the sociology of norms, and agent-based modeling. His current research involves constructing causal models and simulations of vigilante phenomena in Japan during the COVID-19 pandemic.