

Gogolook

2022 Annual Fraud Report

Encompassing Telecommunication, Digital and Web Platforms For the First Time,
Offering Insights on Six Major Global Fraud Scenarios

Supporting Partner: 

Exclusive Data Supplier: **whoscall** | 美玉姨 | **watchmen** | **Chainsight** | 貸鼠先生 | **Constella**

Gogolook

Build for Trust

Gogolook is a leading TrustTech company established in 2012. With “**Build for Trust**” as its core value, it aims to create an AI- and data-driven global anti-fraud network as well as Risk Management as a Service. From multi-communication to fintech, SaaS and Web3, Gogolook creates trustworthy empowerment with the use of technology in various fields.

Gogolook has also teamed up with a number of institutes such as the Taiwan National Police Agency Criminal Investigation Bureau, the Financial Supervisory Service of South Korea, Thai Police Cyber Taskforce, the Fukuoka city government, and the Malaysia police and Selangor state government to fight fraud and ultimately, to build a trustworthy communication network with the largest number database in East Asia and Southeast Asia.

Agenda

- Foreword P. 04
- Calls & Messages Exclusive Data Supplier | **whoscall** P. 05
- Personal Information Leak Co-research Partner | **Constella** P. 10
- Domains Exclusive Data Supplier | **watchmen** P. 13
- Messaging Software Exclusive Data Supplier | **Auntie Meiyu** P. 16
- Cryptocurrency Co-research Partner | **Chainsight** P. 19
- Financial Loan Exclusive Data Supplier | **貸鼠先生** P. 22

No One Is Immune to Frauds.

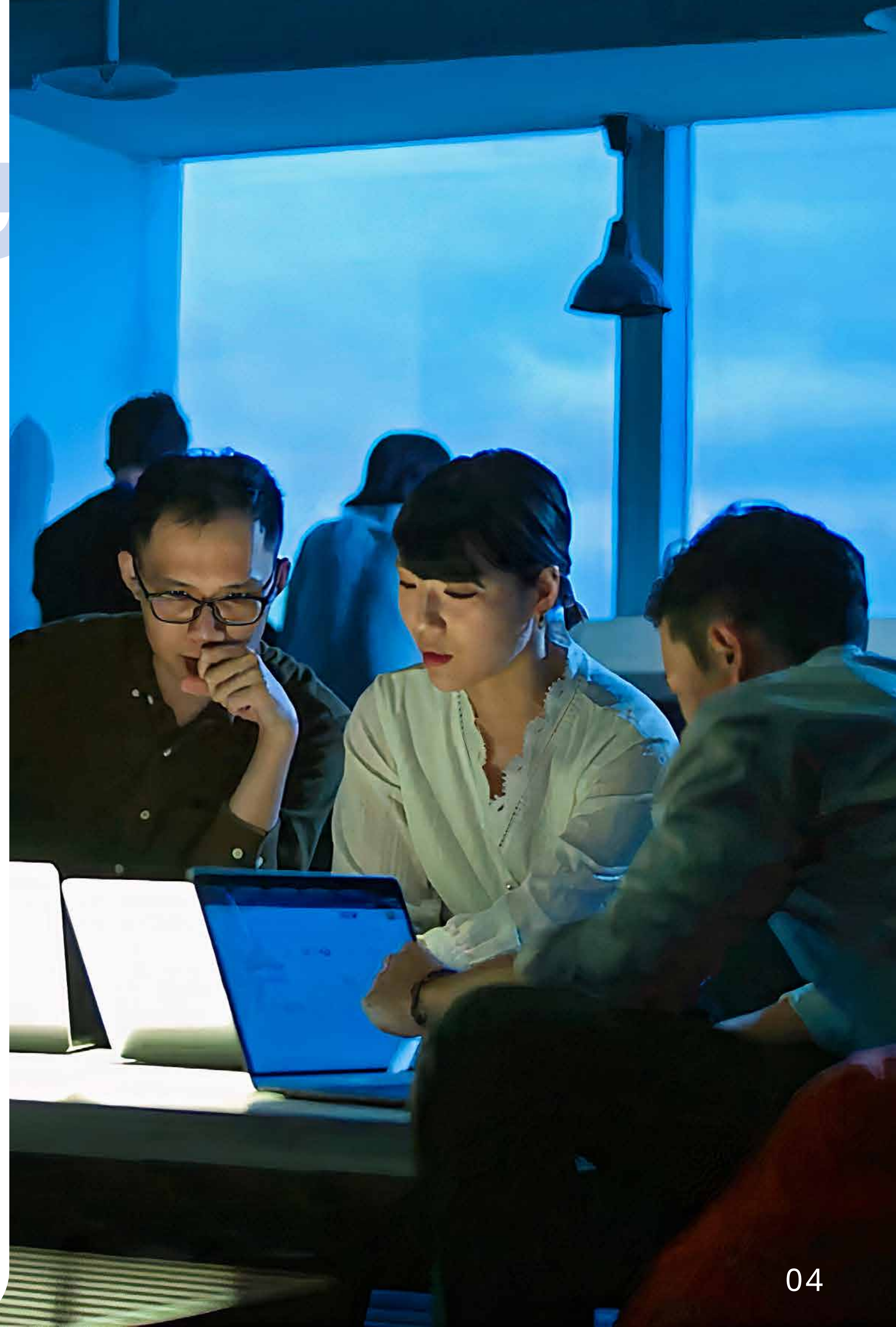
Since Whoscall was developed over a decade ago, Gogolook has been defending against frauds on the front line. Since 2020, Whoscall has been releasing the annual fraud report on the pandemic, phone, and messaging, receiving extensive attention from journalists, users, and enterprises locally and internationally.

Fortune Business Insight estimates that anti-fraud markets worldwide will grow from US\$30.7 billion to US\$129.3 billion between now and 2029, or a 22.8% CAGR. With loopholes in enterprise digital transformation and exponential growth in generative AI in the post-pandemic era, fraudulent technologies and their impacts will exacerbate in the future. In the annual fraud report this year, Gogolook aggregates services and data from its group and strategic partners for the first time. From calls and messages (Whoscall), domain (Watchmen), personal information leakage (Constella Intelligence), messaging software (Auntie Meiyu), cryptocurrency (Chainsight), to financial loan (Roo.Cash), the report analyzes the interconnected fraud market landscape.

Through this report, Gogolook hopes to elevate the public to prevent and identify frauds. According to KBV Research, the global RegTech market size is expected to reach US\$22.3 billion in 2027, at a rate of 19.8% CAGR. Financial Examination Bureau has highlighted “fraud prevention” during inspections at financial institutions. Other government and business organizations should also integrate fraud prevention into their guidelines and ESG measures.



Gogolook Co-founder & Chairman
Jackie Cheng



| **Calls & Messages - Exclusive Data Supplier** |

whoscall

With over 100 million downloads and more than 1.6 billion numbers in its database, Whoscall provides users with unknown number identification, a spam number blacklist, and suspicious message filtering.

The Whoscall team is dedicated to developing fraud prevention technology, utilizing AI technology, and analyzing scam groups. Equipped with this technology, Whoscall is able to display suspicious calls on the screens of users and provide ample warning for malicious calls such as scams, sales, and spam. At the same time, Whoscall is also able to remind users not to miss important calls.

The service originated in Taiwan and expanded to include Korea, Japan, Hong Kong, Thailand, Brazil, Malaysia, and other areas. Whoscall boasts the largest database in East Asia and Southeast Asia.

More about features and services

[Whoscall website](#)

[Whoscall Number](#)

Download **Whoscall** Now!

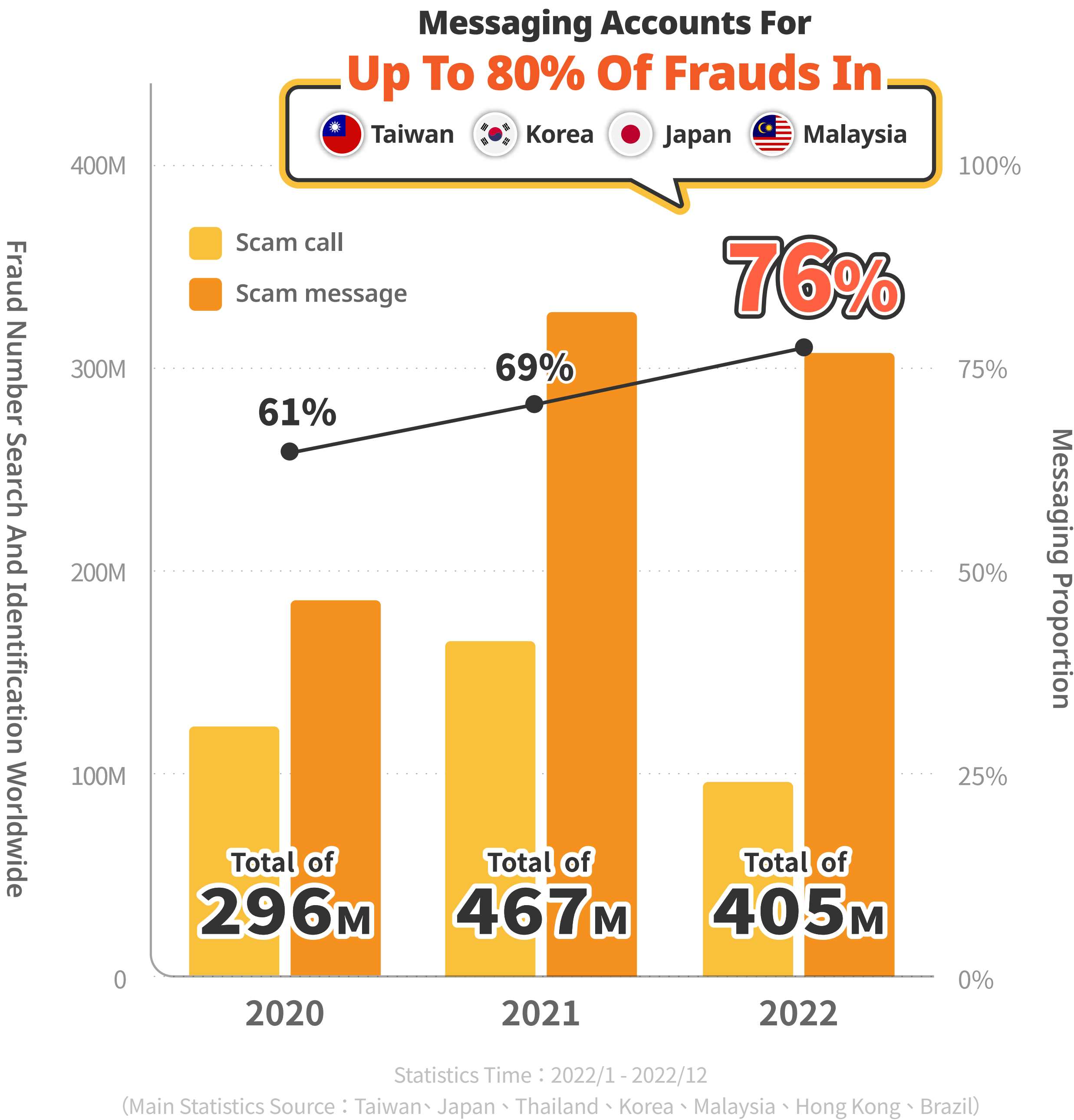


Powered by **Gogolook**

Over 400 million scam calls and messages are circulating worldwide, and text message scams continue to rise

Since online services further popularize under the COVID-19 pandemic, frauds have accelerated across countries in velocity for over two years, without any signs of slowing down. According to Whoscall, a caller ID software, it identified over 405.4 million scam calls and messages for global users in 2022. Even though the number slips by 13%, compared to the previous year, it remains a significant issue. Scammers prioritize text messages for high penetration rates and low costs, so messages account for 76% of “first contacts” in fraud cases, a new record. At the local level, text messages amount to 95% of fraud cases in Japan, and over 80% in Taiwan, Korea, and Malaysia. It shows high consistency among scammers worldwide.







Besides rampant scam messages, Whoscall blocks up to 460,000 short-form scam calls (such as 283617) in Taiwan a year, tripling from the previous year. Scam calls via VoIP systems (starting with +886) often pretend to be bookstores (such as books.com, eslite, and kingstone), and social welfare organizations (such as World Vision, Eden Social Welfare Foundation, and Huashan Social Welfare Foundation). Under the threat of personal information leakage, scammers acquire consumption records, and increase scams by multiple folds. People should be particularly mindful.



Compare scam tricks and anti-fraud policies in different markets

Under these threats, anti-fraud industries will grow to US\$129.2 billion in market scale by 2029, or a 22.8% CAGR, according to Fortune Business Insight. Frauds have also localized with unique formats and hotspots. Based on fraud search and identification (calls and messages included) per capita among Whoscall users, Thailand tops the list with 33.2 times on average annually. This figure underlines the severity in fraud threats. With the first surge of scamming messages in Hong Kong, fraud cases have increased in multiple folds. In comparison, numbers in Taiwan and Korea decrease slightly.

According to the research by Whoscall global team, scam messages closely follow local current affairs. For instance, after Taiwanese government decided to refund citizens for overtaxing, related scam messages emerged right away. Scammers in Thailand centered on the social network TikTok due to its rising popularity. In Hong Kong, scammers pretended to be public security officers from China. To fight against frauds effectively, governments have drafted anti-fraud policies, established designated authorities, and mobilized private companies and celebrities to raise anti-fraud public awareness. For example, Thailand and Malaysia have deployed new reporting systems, similar to the 165 hotline by Criminal Investigation Bureau in Taiwan. Korea has instructed prosecutors to set up anti-fraud teams across ministries. Japan launched an anti-fraud campaign with top-notched celebrities to successfully expand its reach and impacts. In these anti-fraud systems, Whoscall and other innovative applications also play a key role.

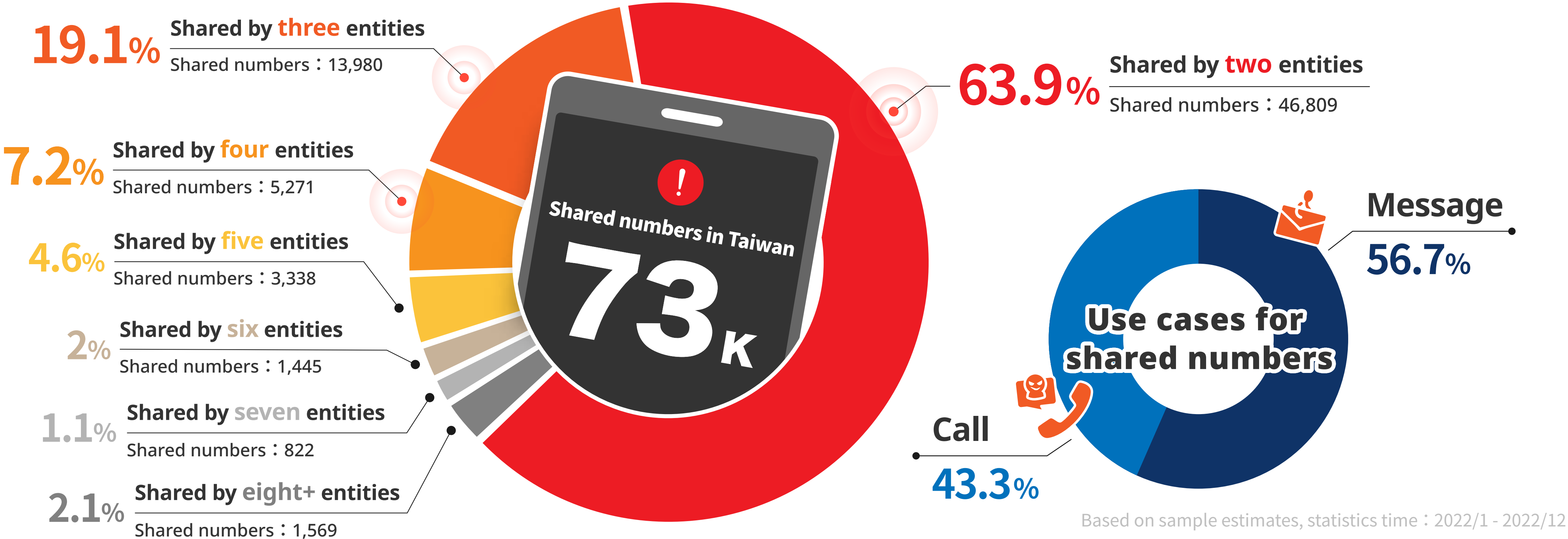
	Fraud search and Identification per capita / YoY (calls and messages included)	Emerging scam types	New official anti-frvraud policies
 Taiwan	17.5 ↓ (-20%)	Phishing text messages for 6000 tax refunds in the name of national taxation bureau	<ul style="list-style-type: none">• Administrative Yuan announces action guidelines against new-generation fraud strategies• Financial Supervisory Commission includes anti-fraud in the key tasks of the year
 Thailand	33.2 ↑ (+7%)	Phishing text messages and calls for tiktok event prize notice	<ul style="list-style-type: none">• Royal Thai Police sets up fraud report hotline 9777• Thailand Post works with Whoscall to enhance anti-fraud capacities in non-capital regions
 Japan	5.8 ↑ (+5%)	Investment and sale contract scams targeted young people, after adulthood is expanded to people over 18	<ul style="list-style-type: none">• National Police Agency continues on anti-fraud SOS47 campaign to work with top-notched celebrities
 Malaysia	16.5 ↑ (+15%)	Inquiries to receive otp authentication codes with false claims of smartphone malfunctions	<ul style="list-style-type: none">• National Scam Response Centre sets up report hotline 997• Royal Malaysia Police exclusively works with Whoscall to enhance fraud number databases
 Korea	5.3 ↓ (-23%)	Fake college admission notices to young people for personal information	<ul style="list-style-type: none">• Supreme Prosecutors' Office establishes a joint investigation team with police, Financial Supervisory Service, and Korea Communications Commission against frauds
 Hong Kong	11.9 ↑ (+231%)	Fake law enforcement scams in the name of chinese national security officers	<ul style="list-style-type: none">• Hong Kong Police Force launches Scameter for the public to check scam numbers, accounts, and websites

Statistics Time : 2022/1 - 2022/12

Over 70,000 shared phone numbers in Taiwan may breed scams and jeopardize brand reputations

Phone calls and text messages are still main contact channels for various occasions. From service applications, bank notices, business development, job interviews, to restaurant reservations, these purposes all require phone communication. Text messages are widely used for OTP verification and customer relationship management. To reduce costs, some companies and government bodies choose VoIP or mass text message distribution services. As a result, the same number may be used for cram school class promotion calls, OTP verification, and pornography messages.

Whoscall data show there are over 70,000 shared phone numbers in Taiwan, and each number may be used by two to over a dozen entities. Behaviors among these numbers, 56.7% are used to send text messages, and 43.3% are used for phone calls. Considering risks with shared numbers, Whoscall suggests corporations and government bodies apply or register verified numbers, to avoid frauds or tainted reputations.



| **Personal Information Leak - Co-research Partner** |

Constella

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to safeguard what matters most and defeat digital risk.

Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your executives, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

For more information about **Constella Intelligence** services contact **Gogolook** partners

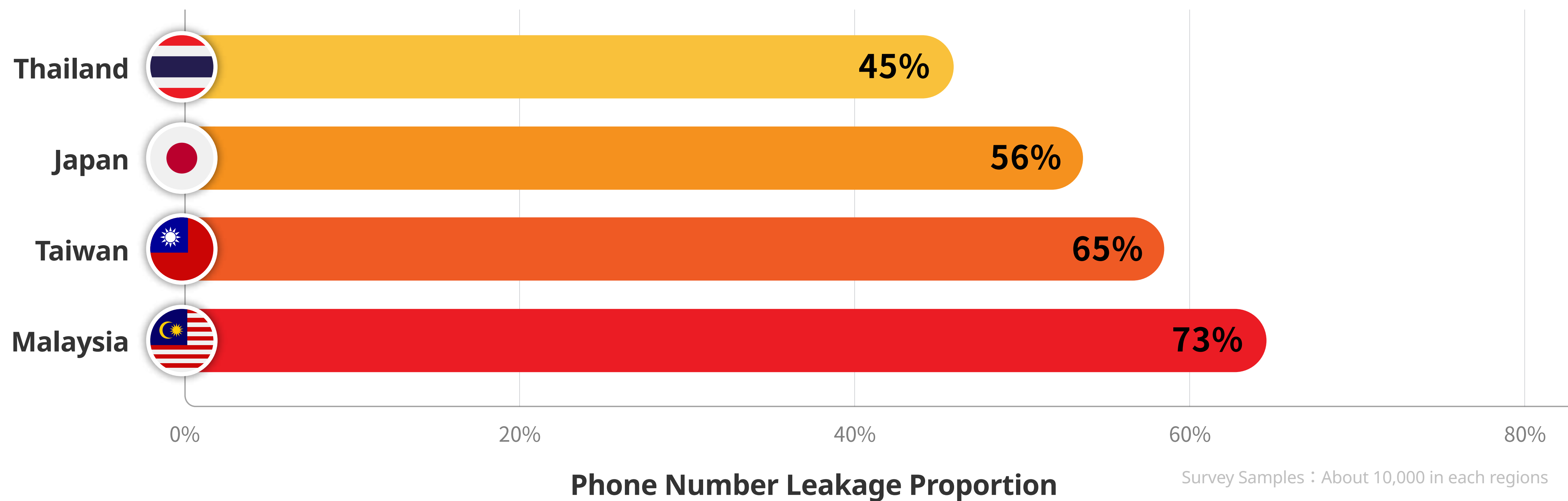
business@gogolook.com

Partner with **Gogolook**

Gogolook estimates that phone numbers of up to 10.4 million people in Taiwan have been leaked to scammers, disclosing the upstream reality in the scam industry

Private information leaks are often the first step for scammers to access contact details before their attacks. Leaks can happen when enterprise or government databases are hacked, or when users fill out questionable surveys, psychological tests, or forms on phishing sites. To minimize threats from the start, Gogolook, the developer behind Whoscall, collaborates with Constella Intelligence, an international digital risk protection service provider, to analyze phone number leaks in several major markets, including Taiwan.

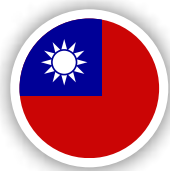



Results show that 75% of phone numbers in Malaysia are leaked, followed by 65% in Taiwan. Up to 56% of phone numbers in Japan are leaked. For estimated 16 million people aged 20 to 65 in Taiwan, according to Department of Household Registration data, it means phone numbers of 10.4 million people are maliciously leaked or sold. It underlines the importance of anti-fraud and Whoscall installation. In comparison, leakage rates in Korea is only 15%, with much better security than neighboring countries.



Which category of personal data leak was the worst? Gogolook: Login passwords, phone numbers, and names are most leaked private information in Taiwan

Personal Data Protection Act is designed to protect name, birthday, fingerprint, sex life, healthcare history, criminal record, and other directly or indirectly identifiable data. Private data stored in public and private sectors may be mismanaged and accessed by third parties for leaks. Gogolook has looked into which personal information is leaked more often in each market. It's a reminder to pay more attention to potential breaches.

In Taiwan, Thailand, and Malaysia, top three leaked items are all login password, phone number, and name. For 4th to 7th places (nationality, email, address, and birthday), three markets are slightly different in order. In Japan and Korea, name, login password, and phone number are top three in the list. Each piece of leaked information will lead to different risk scenarios. For example, after login passwords are leaked, online banking or social network accounts can be stolen. When scammers access names, phone numbers, and even payment and shopping records, they can easily initiate phone and message attacks. If names and addresses are leaked, people may soon receive “unsolicited packages with payment request on arrival”. People are encouraged to choose two-step authentication in online services, change strong passwords regularly, and identify phone calls and messages with Whoscall.

	 Taiwan	 Thailand	 Malaysia	 Japan	 Korea
1st	Password	Password	Password	Name	Name
2nd	Phone Number	Phone Number	Phone Number	Password	Password
3rd	Name	Name	Name	Phone Number	Phone Number
4th	Country	Country	Address	Country	Country
5th	Email	Address	Country	Address	Address
6th	Address	Date of birth	Date of birth	Email	Email
7th	Date of birth	Email	Email	Date of birth	Date of birth

Survey Samples :
About 10,000 in each regions

| Domains - Exclusive Data Supplier |

watchmen

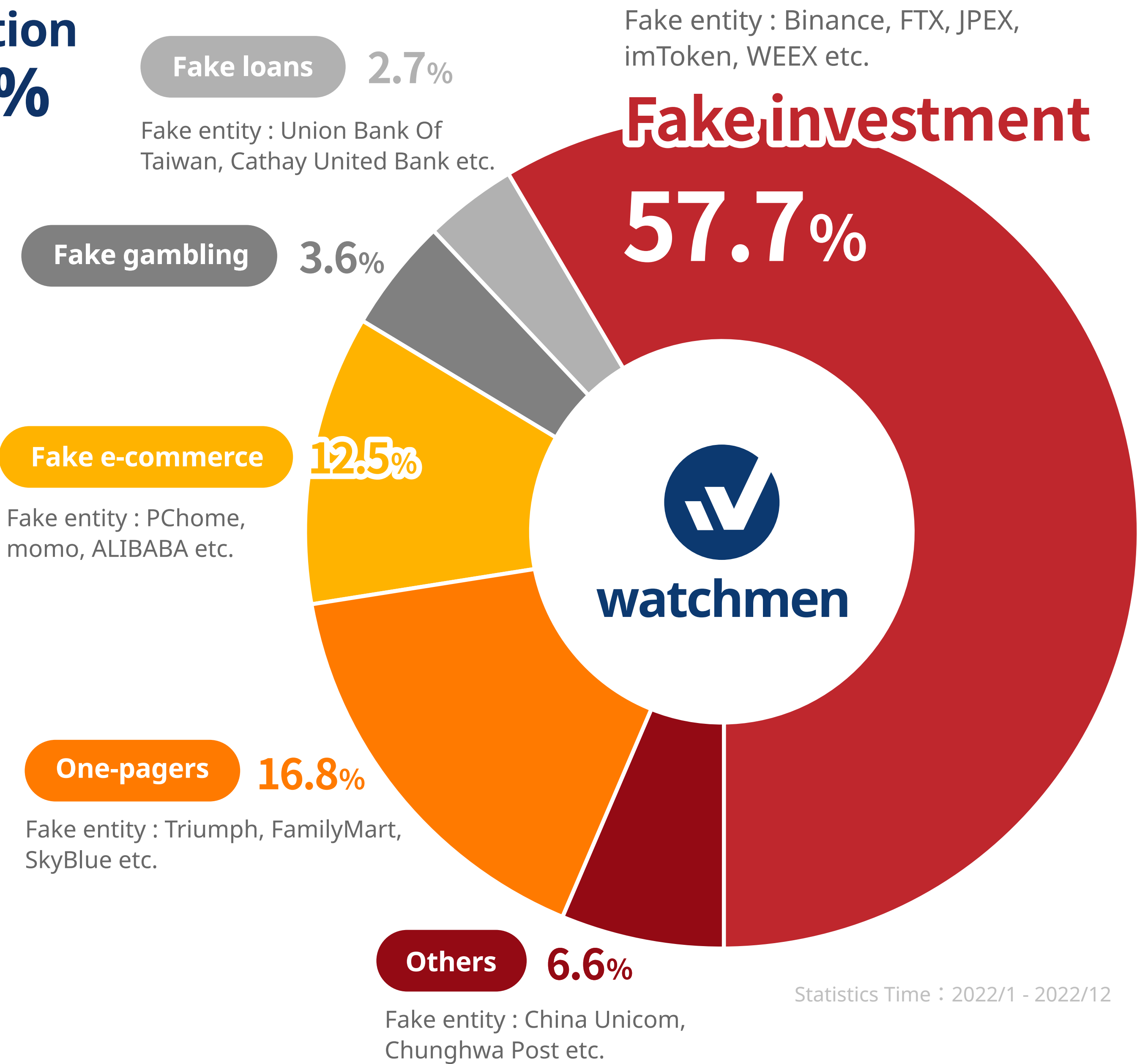
Watchmen Reputation Protection Service is a Gogolook solution comprising Whoscall Number and Fraud Early Warning System. It monitors and analyzes communication channels (e.g. phone calls, SMS, websites, social media platforms) between enterprises and customers. The service activates anti-fraud mechanisms immediately when a fraud or scam against an enterprise is detected, further strengthening protection against digital risks and of consumer rights with the one-stop service.

More about **Watchmen Reputation Protection Service** features

Over 2,000 new fraudulent domains are created monthly! Watchmen Reputation Protection Service reveals nearly 60% are related to investment

With Whoscall Numbers and Fraud Early Warning System, Gogolook Watchmen Reputation Protection Service deploys designated systems and teams for enterprises to detect fraudulent information in text messages, calls, domains, and social networks in real time. In response, companies can initiate anti-fraud mechanisms immediately. Fraud cases now often spread fraudulent domains and websites via text messages, messaging apps, and social media to trick victims. At the end of 2022, Watchmen worked with Criminal Investigation Bureau to develop an AI system to detect fraudulent domains. Through this effort, scam websites will be detected and blocked before spreading.

According to Watchmen analyses, over 2,000 new fraudulent domains are created monthly on average. These scams are broadly in several categories: investment (57.7%), one-page websites (16.8%), e-commerce (12.5%), gambling (3.6%), loans (2.7%), and others (6.6%). For different subjects, scammers will produce website lookalikes from known brands to lower user alerts. For example, fake investment websites imitate cryptocurrency exchanges, such as Binance, FTX, and JPEX. Fake e-commerce platforms look similar to PChome or momo. Fake loan websites are often named similarly after renowned banks to be confusing, such as Cathay Loans or Far Eastern Finance Marketing Center.



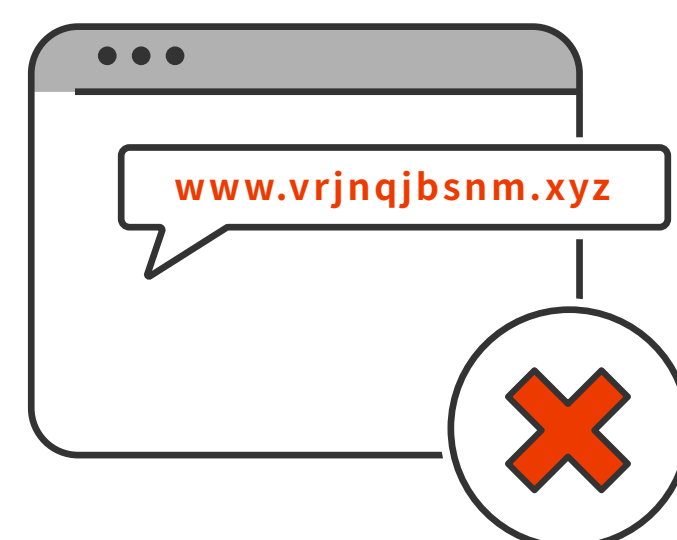
Watchmen pinpoints four common features among fraudulent domains

Administrative Yuan has announced action guidelines against new-generational frauds, and highlighted efforts to identify, block, intercept, and penalize frauds. People should be equipped with knowledge to identify scam tactics. According to Ministry of the Interior, most common scam tricks in 2022 are fake online sales, fake investment, and installation cancellation, in which fraudulent domains are critical. Among proliferating fraudulent domains, some features remain the same. After analyzing thousands of cases, Watchmen has compiled four features for public attention.



01 Amateur Web Design

Images in low resolutions, texts in Simplified Chinese, shabby pages with broken buttons and menus.



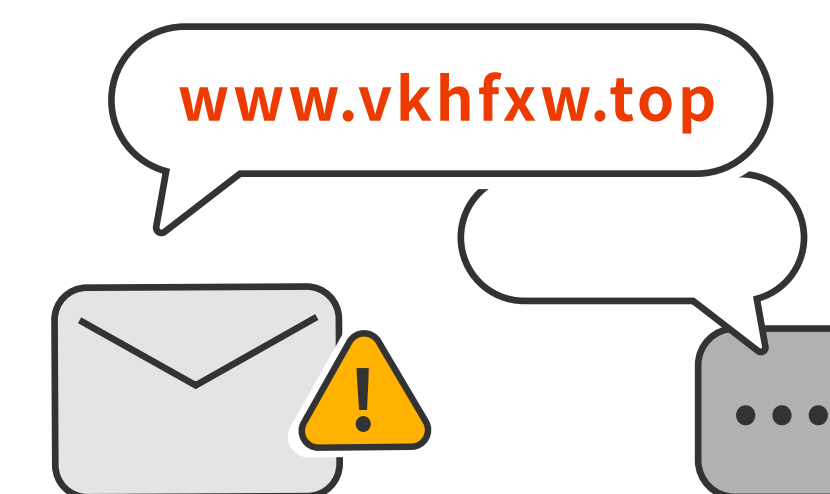
02 Suspicious Random Domain Names

Instead of common legal domains, such as .com, .net, .org, or .tw, irregular spellings or confusing names are alarming.



03 Newly Registered Domains

Use WHOIS databases to search when domains are registered, as fraudulent domains are mostly registered within three months.



04 High-risk Distribution Channels

Fraudulent domains are unlikely to appear in Google research results, and they are mainly distributed through text messages, LINE/Telegram groups, or advertisement/groups on social media.

| Messaging Software - Exclusive Data Supplier |



Auntie Meiyu

Auntie Meiyu is an AI-powered fact-checking chatbot. It automatically compares suspicious information, such as text messages, rumors in graphs, unknown phone numbers, phishing links, virtual asset wallet addresses, and LINE ID, with various fact-checking platforms, law enforcement authorities, and security databases.

Users can obtain results based on multiple sources in real time, without falling victims to scams.

More about **Auntie Meiyu** features and services

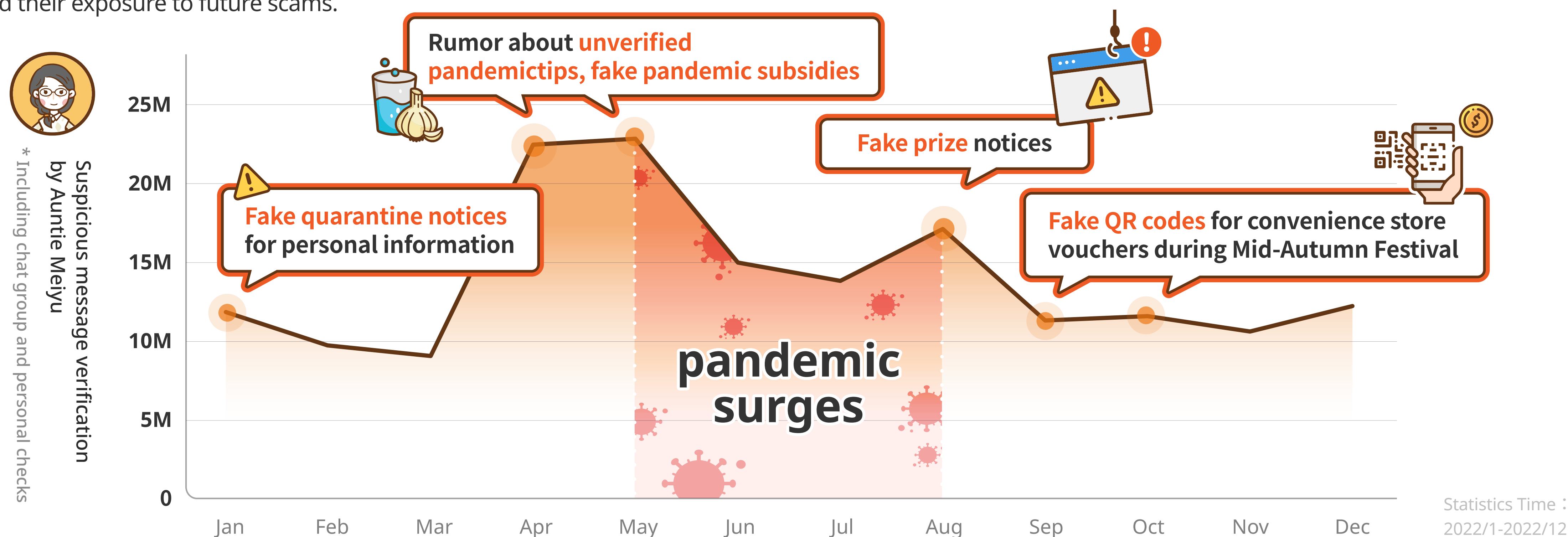
Add **Auntie Meiyu** as your friend on LINE now

Auntie Meiyu

Auntie Meiyu highlights receding pandemic-related scams and new emerging tactics via messaging software

As communication technologies popularize, rumors and scams have proliferated via messaging software, including LINE and Telegram. Gogolook's AI-powered fact-checking chatbot Auntie Meiyu has been adopted by over 520,000 users. In 2022, it was recommended by Central Election Commission and Taiwan Centers for Disease Control. According to its latest data, Auntie Meiyu verified/debunked suspicious information for 1.67 million times in 2022. Scammers constantly modify their tactics and phrases along with current affairs in Taiwan.

Scams via messaging apps last year still centered around the pandemic. During the surge in May to August last year, according to Taiwan Centers for Disease Control, questionable information also peaked in the same period. Criminals distributed unverified pandemic prevention tips and fake links for pandemic subsidies. They took advantage of uncertainties for illicit profits. Starting from August, though, many fraudulent one-pagers emerged that plagiarized CPC, FamilyMart, and 7-ELEVEN websites. Around Mid-Autumn Festival, scammers randomly mailed fake paper vouchers with QR codes in the name of convenience stores. Voucher photos also spread widely via messaging software. By scanning QR codes on these invalid vouchers, users immediately friended fraudulent accounts, and increased their exposure to future scams.



Auntie Meiyu warns fake LINE authentication and Google Forms as new personal information risks

According to AI-powered fact-checking chatbot Auntie Meiyu, over 14,000 fraudulent links were detected in 2022. Besides fraudulent domains for investment or loans, Auntie Meiyu also pinpoints two new types of scams via messaging software, including fake LINE authentication and Google Forms for personal information.

Scammers often apply fraudulent accounts on messaging apps. Many people have been pulled into unknown groups by large numbers of fraudulent investment advisor accounts. These accounts also disguise as friends, family members, or brands, and ask for LINE authentication. When careless users follow instructions to submit personal information, such as phone numbers, passwords, or authentication codes in text messages, their accounts are more likely to be stolen by others with hostile intents. Another type of scams is exercised with Google Forms. Scammers use free Google Forms to produce surveys with product trials or loan applications for distribution. It is difficult to verify authenticity, and easy to cause personal information leakage.

Auntie Meiyu also reminds that prize scams and free sticker scams were still rampant last year via messaging software to steal person information. Auntie Meiyu can verify suspicious links, messages, or wallets. Do not click on questionable links, do not give away personal information easily, and do not download suspicious applications.



| Cryptocurrency - Co-research Partner |

Chainsight

Chainsight helps companies and users detect web3 risks and provide insights for every crypto transaction. Our AI-powered fraud detection solution has already protected about 300 million end users, including cybersecurity and anti-fraud companies like Trend Micro and Gogolook. We have received global recognition from G20, the Bank of International Settlements, the New York State Department of Financial Services, and the Japan Financial Services Agency, and have been invested by Y Combinator, Samsung NEXT, and Franklin Templeton. Our team of cybersecurity, AI, and blockchain experts from Massachusetts Institute of Technology (MIT) and Carnegie Mellon University ensures our customers receive outstanding protection against web3 attacks.

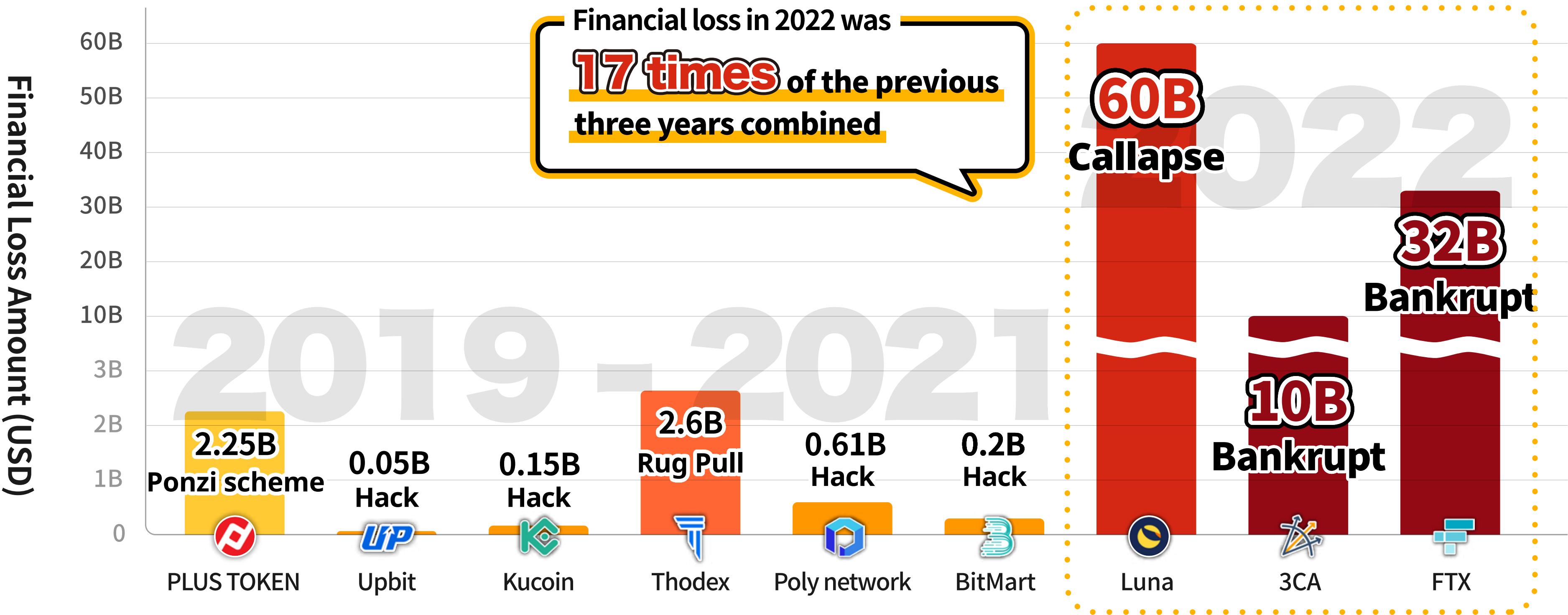
Chainsight API offers extensive coverage, monitoring over 10 blockchains, 300 thousand dapps/NFT/tokens, 105 million phishing sites, and approximately \$58 billion dollars worth of daily crypto transactions in real-time. Our customer-centric approach offers any crypto and internet companies to mitigate crypto scams on their platforms. We are actively working towards integrating with social media, messaging apps, search engines, telecommunications and phone companies to secure the next billion users across web2 and web3 globally.

More about **Chainsight** features and services

Partner with **Gogolook**

With skyrocketing investment losses, Chainsight: Cryptocurrency losses reached over US\$100 billion last year, 17 times of those in the previous three years combined

As blockchain industries prospered, cryptocurrency market values worldwide also skyrocketed to US\$2.7 trillion in 2021. According to Chainsight, a blockchain data analytics startup that was selected into Y Combinator in Silicon Valley last year, major investment losses and scams around cryptocurrency also grow significantly. Financial losses in 2022 were 17 times of those in the previous three years combined. In 2018, the Ponzi scheme of Plus Token and the rug pull of Thodex caused US\$2.25 billion and US\$2.6 billion of investment losses respectively. In May 2022, LUNA, one of the top ten cryptocurrencies, crashed in three days. It indirectly led to two bankruptcies in June and November: Singaporean cryptocurrency hedge fund Three Arrows Capital and the second largest cryptocurrency exchange in the world FTX. Each major incident triggered over US\$10 billion of financial loss, and more than US\$100 billion throughout the year. FTX founder Sam Bankman-Fried faced multiple charges on asset appropriation and fraud. Digital asset management platform Steaker in Taiwan was also jeopardized in the process, and its founder was put into custody for potential Banking Act violations. Multiple cryptocurrency organizations have filed for bankruptcy in a short time-frame after crises, so their circulation and investment risks have attracted attention from supervisory authorities in many countries.



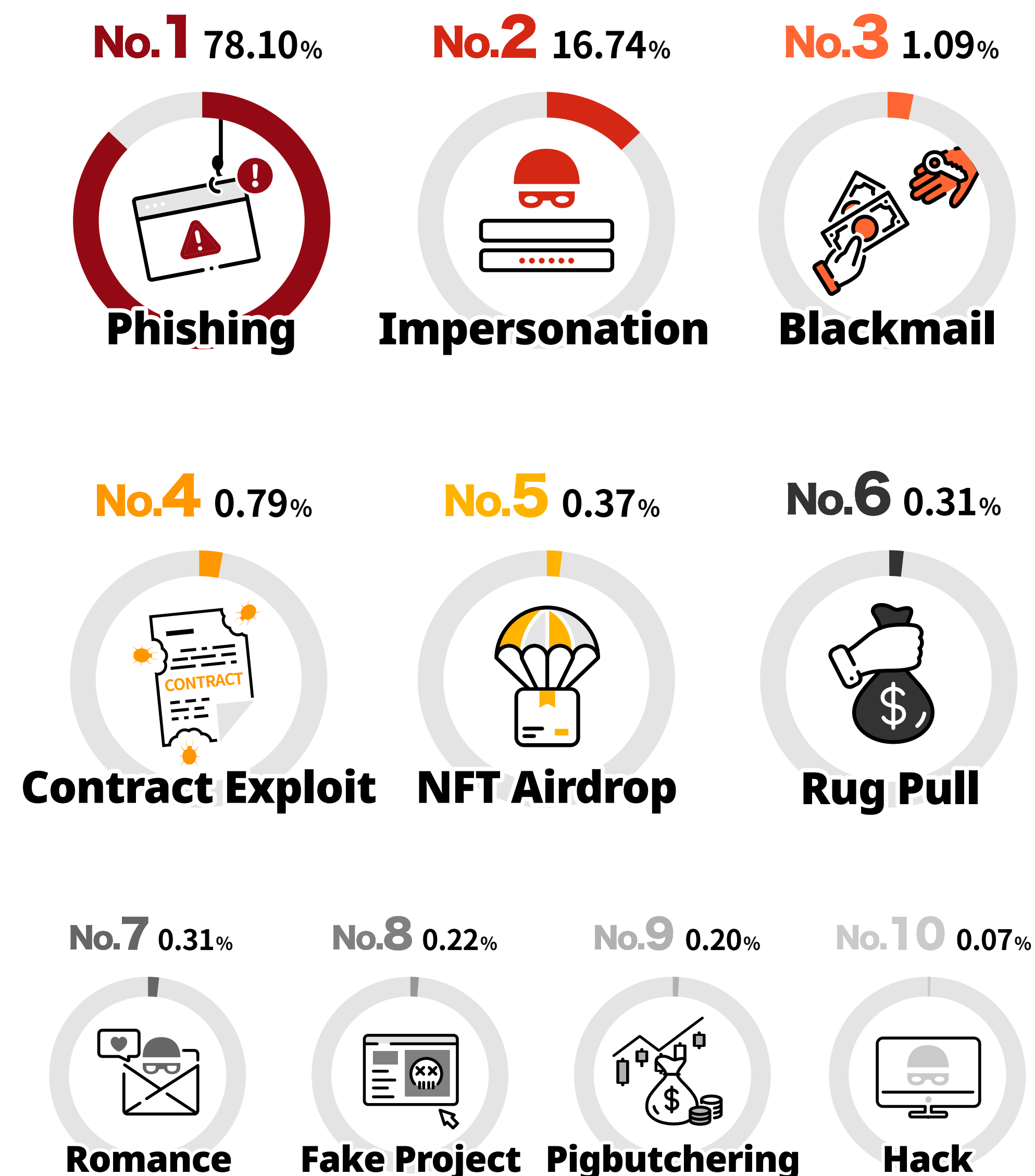
Statistics Time :
2019/1 - 2022/12

Chainsight discloses ten cryptocurrency risk loopholes, in which phishing accounts for nearly 80%

Besides losses incurred by stablecoin structural design and governance loopholes, cryptocurrency frauds and security loopholes continue to happen under the radar via social media and messaging software. Chainsight includes criminal transaction data over ten years in its blockchain database, and utilizes AI to construct virtual asset trade risk forecast and identification services. It covers 10 public chains, over 300,000 curries, and NFT.

According to Chainsight statistics, phishing accounts for nearly 80% of frauds. Fraudulent domains are one of the most common tactics. With special domain names with cryptocurrency websites, it is very easy to be confused with similar domains in different orders or suffixes. Even for senior users, it is sometimes difficult to immediately evaluate the authenticity, whether wallets or exchange applications are downloaded from fraud websites, or wallet access is obtained through fraud websites. Fake identity is the second common tactic (17%). Scammers pretend to be official representatives from exchanges or cryptocurrency operators in emails, websites, social networks, or messaging software. They request for personal sensitive information, such as wallet backup phrases, API keys, private keys, and password reset authentication codes, to steal private assets. Based on various risk types, it indicates frauds and risks related to cryptocurrency are much more diverse and complex, compared to traditional investment. Examples include blackmail, smart contract loopholes, and NFT airdrops. Even though these cases are proportionally fewer, they can still create huge economic losses to investors.

As a guardian to blockchain trade security, Chainsight reminds users to take precautions measures to protect personal digital assets. Chrome extension Web3Check supported by Chainsight is available for free download to detect trading websites and cryptocurrency wallet addresses in real time. In the future, Chainsight will add warnings to exchange circulation. When abnormal cashflows happen to exchanges, Web3Check will inform users right away to protect digital assets in real time.



| Financial Loan - Exclusive Data Supplier |



貸鼠先生

Roo.Cash, a Gogolook fintech brand, has partnered with numerous banks to provide real-time comparison of diverse financial instruments, including credit cards, loans, digital accounts, and mortgage.

The big data-driven service offers personal financial analysis and calculators for monthly credit loan and mortgage payments based on latest interest rates. In addition, the 1-1 live customer service is available to further complete the one-stop financial service.

More about **Roo.cash** features and services

Stay alerted to common scam tactics and loan frauds on social media ads, LINE, and text messages

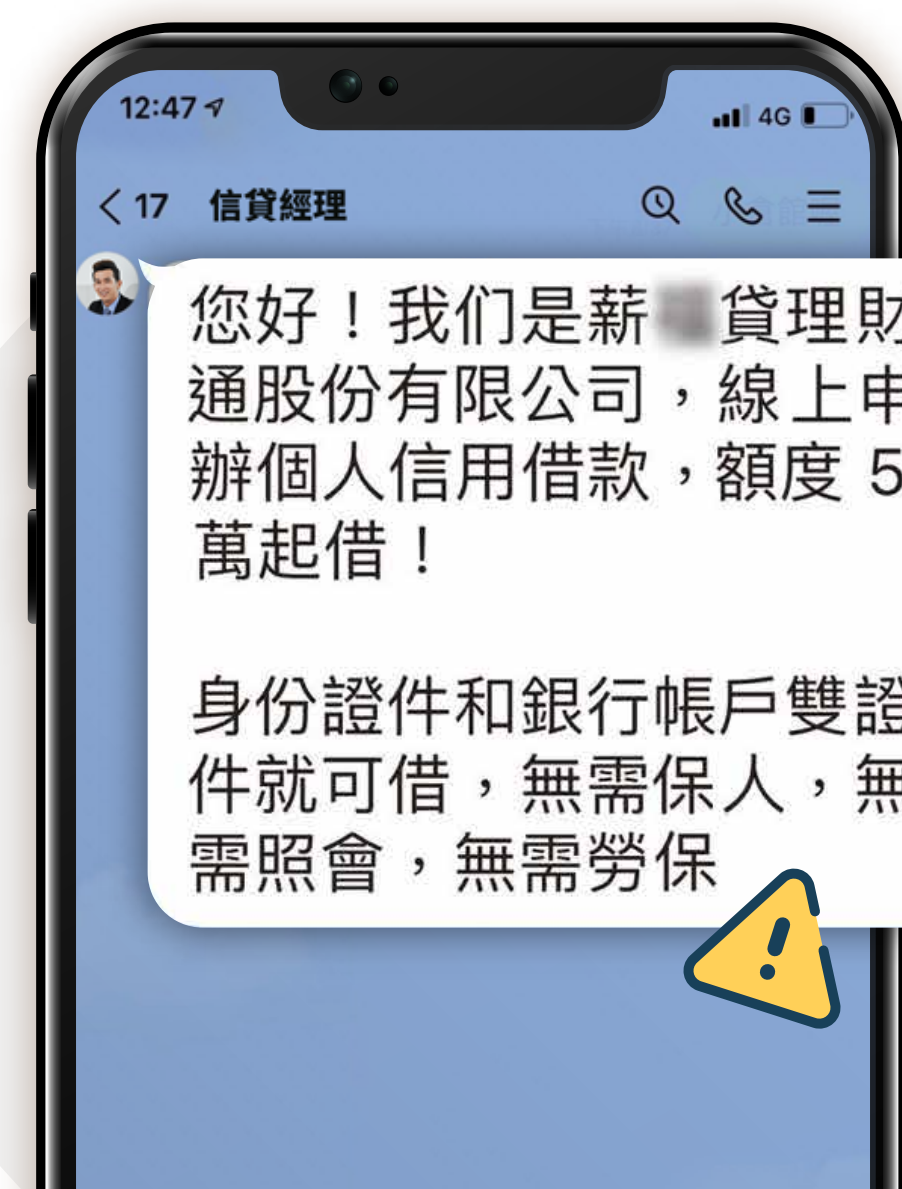
Rising interest rates in recent years cause global economic downturns. However, up to six million people in Taiwan face challenges to access banking services, without sufficient credit records or income certificates. Scammers and loan sharks take advantage of urgent financial needs among the unbanked communities, and distribute fake installment loans or small-amount credits via multiple channels. These fraudulent messages often lure victims into scams. According to Gogolook's financial product comparison platform Roo.Cash, Facebook/YouTube ads, LINE accounts, and unsolicited text messages are three major channels for loan frauds to attract victims.

Roo.Cash also lists common scamming processes. Through these channels, loan frauds direct victims to scam websites and apply for loans. In submitting, reviewing, and approving the loan, they insert scam tactics, such as claiming wrong account information for security deposits and thus asking for payment to reactivate the process. Roo.Cash urges people with credit needs to access legal products and solutions, in order to avoid scams.

1 Social Media Ads



2 LINE Fake Account



3 Unknown SMS



Get no money but sued? Roo.Cash discloses 5 key features for loan fraud sites

Criminal Investigation Bureau statistics show 574 loan frauds by the end of October 2022, a 77% increase compared to 2021. It indicates public anti-fraud literacy remains insufficient. To elevate public awareness, financial product comparison platform Roo.Cash analyzes common scam tactics and lists five features in loan frauds.

1. Resemblance: Scammers often plagiarize official websites and logos from renowned banks, and distribute information via text messages, ads, and fraudulent Facebook pages. People mistake them as parts of particular banks.

2. Not in search results: It is unlikely to find any basic information behind loan frauds, such as landline phone numbers, registration addresses, or company representatives. Remember to check before act.

3. Personal ID requirements: If you submit personal documents as requested for loans, such as seals, passbooks, ATM cards, ID cards, and natural personal certificates, you are likely to be criminalized, and become dummy accounts for scammers.

4. Loan guarantees: Many scammers fraudulently claim loan guarantees or abundant precedents.

5. High amounts: Scammers often fraudulently offer very high amount of credits without collaterals or credit records. In the process, though, they will request account reactivation fees, risk unlocking charges, processing fees, or security deposits, but never deliver credits.



Resemblance

Names similar to renowned banks, and distribution loan information via ads or social media pages.



Not in Search Results

Cannot find basic business information, such as landline number, registration address, and company representative.



ID Requirement

Request to submit seals, passbooks, ATM cards, ID cards, or natural person certificate.



Loan Guarantee

Claim 100% guarantee or abundant precedents.



High Amount

Claim very high credit amounts without collaterals or credit history.

Gogolook

Build for Trust

For business and marketing partnership, contact : 02-7752-0996 #102 | business@gogolook.com | www.gogolook.com