Residents need effective alerts against cyberfraud

Online fraud exploits fake e-commerce, job offers, dating, and the lure of inflated profits. Artificial intelligence identity theft can swap faces and mimic voices to dupe the elderly, new mainland arrivals, and foreign students. Internet-savvy syndicates operate across borders to scam the gullible. **Oasis Hu** investigates.

The number of fraud cases increased alarmingly over the last decade, despite alerts from the authorities. Between 2012 and 2022, the number of fraud cases in Hong Kong rose 303 percent — from 6,923 to 27,923 cases. In the first quarter of 2023, scams at 8,866 cases, rose 65 percent compared with the same period last year. Fraud constituted 43 percent of all crimes reported for the period.

The consequences can be devastating: many lose lifetime savings, suffering emotional trauma. In the first four months of this year, in investment fraud alone, Hong Kong lost more than HK$700 million ($89.6 million) — a more than 50 percent increase above the same period last year. Measures to protect unsuspecting residents are inadequate. Much more effective communication and education is urgently needed.

In response to China Daily, the Hong Kong Police Force confirmed it plans to conduct concentrated anti-fraud publicity campaigns in the second half of this year, targeting vulnerable communities.

The HKPF will also coordinate with sectors such as banking, finance and telecommunications, to raise fraud awareness, and to encourage fraud prevention measures by residents.

Growth in online fraud

In early 2023, the HKPF reported a significant fall in 2022 of selected major crimes, including burglaries, robberies, arson, snatching, etc. But the overall number of crimes reported in 2022 rose 8.7 percent to 70,048 cases.

This trend was mainly caused by the increase in the number of deception cases — in 2022, the number of such cases rose significantly to 27,923, an increase of 45.1 percent from 19,249 in 2021, involving HK$ 4.8 billion.

Of the reported fraud cases, approximately 70 percent, nearly 20,000, were internet-related. The most prevalent were scams of online shopping (8,735 cases), online employment (2,996 cases), online investment (2,850 cases), and online romance (1,533 cases).

The number of online romance fraud cases in 2022 represented a 158 percent increase since 2019, at HK$700 million, a rise of HK$500 million over 2019. More than 80 percent of the victims of online romance scams in 2022 were women.

Apart from online fraud, telephone fraud has been widespread in recent years, with case numbers rising 360 percent from 615 cases in 2018 to 2,831 cases in 2022, involving more than HK$1 billion.

Fraudsters impersonating officials or law enforcement, cheated victims out of their personal data or money in 54 percent of telephone scams in 2022, involving losses of HK$960 million. In these cases, most victims were nonlocal residents: students from the Chinese mainland, or foreign students studying in Hong Kong.

The remaining phone scams were "guess-who-I-am" tricks, where victims are led to believe the caller is a relative or friend urgently needing money. This type of fraud resulted in losses of $110 million in 2022, and most of the victims were elderly people aged 60 or above.

Beyond Hong Kong

The surge in online fraud is a global phenomenon. Singapore experienced a 32.6 percent increase in fraud cases between 2021 and 2022, while Taiwan recorded a 21 percent increase.

Most reported fraud cases in the world were online. Globally, online shopping scams, investment scams, and job search scams were among the major categories of fraud, similar to the Hong Kong experience.

Solicitor Bob Yan Xianming attributes the global surge in fraudulent activities to the accessibility and convenience of the internet.

The ease with which people can send messages online and acquire fake social media accounts, phone numbers, and bank accounts at minimal cost, have made this crime simple and inexpensive to execute, said Yan.

Internet and telephone fraud can target victims across borders. Internet fraud technology continually evolves, responding to threats, making it difficult to trace, combat, or arrest criminals. However, the 45 percent surge in Hong Kong since 2021 ranks among the highest globally.

Anita Chow Cheuk-ying, a partner at local law firm Morley Chow Seto, and an experienced fraud case litigator, said the so-called "Hong Kong scam" does not only involve victims or perpetrators in Hong Kong, but also other regions, such as the United States, Malaysia, Japan, and Singapore. Because defrauded money was transferred to Hong Kong, or sent elsewhere through Hong Kong, victims had to seek legal services or call the police in the city.

No exchange controls

Echoing Chow's statement, Yan said that Hong Kong's absence of exchange controls enables swift money transfers, making it a favored destination for fraudsters. Also, the process of starting a company in Hong Kong is relatively simple, making it easier for scammers to defraud people using the names of shell companies, said Yan.

"Free trade is a defining characteristic of Hong Kong as an international financial hub. If financial controls are too strict, it could dissuade businessmen from investing in the city, but if the controls are too lenient, it could pose risks," Yan said, adding that combating scams in Hong Kong requires a balance between freedom and security.

Francis Fong Po-kiu, honorary president of the Hong Kong Information Technology Federation, attributed the growth in fraud cases in 2022 to an increase in online activities such as shopping, dating, and investment during the COVID-19 pandemic. The pandemic introduced the elderly to the internet for the first time. They became easy targets for scammers, said Fong, as they continued using the internet after the pandemic as it is convenient.

Psychological manipulation

Private investigator Yiu Man-ho, is president of the Global Anti Scam Association, a local organization educating people about scams and how to combat fraud. Yiu noted that while most people are cautious when asked for personal information or money, scammers can manipulate victims' psychological states, causing them distress, and to behave irrationally.

Building trust is the first step in the scam, said Yiu. Online romance fraudsters are skilled at meeting their victims' emotional needs and can spend months, or even years, cultivating a relationship. They often please their victims with gifts and money, to build trust before committing fraud, explained Yiu.

Trust also plays a significant role in business fraud. Many victims of business fraud are cheated because they believe they are dealing with a familiar partner, said Chow. Then scammers may create bank accounts or email addresses closely resembling the real ones that victims are familiar with, to exploit their trust.

According to Fong, creating anxiety is a way for scammers to manipulate victims. In telephone scams, scammers impersonate government officers to pressure the victim to transfer money, even threatening that the victim will be arrested by the police if money is not received promptly.

In addition to inducing anxiety, Fong noted that scammers can also appeal to victims' greed. In online investment cases, they may offer money or promise a significant return on investment first, before luring the victim into the big hit.

Yiu noted that many scam messages in recent years closely track the public's daily lives and government policies. During the pandemic, there were more scam messages about the government giving out consumer coupons.

Similarly, during the "Happy Hong Kong" promotional activity to attract tourists by offering air tickets, there were multiple scam messages promising free air tickets. After the pandemic, due to the economic downturn and job losses, people seek additional sources of income. This mindset can be easily exploited by scammers, said Yiu.

Combating online fraud

"Combating fraud is never an easy task," admitted Fong. The Real-name Registration Programme for Subscriber Identification Module (SIM) Cards Hong Kong implemented on March 1, 2022, requires that all users should complete real-name registration for their SIM cards with their telecommunications service providers by Feb 23. Within two months after the deadline, the police arrested four people using false identities for SIM registration and seized 65,000 telephone cards.

It is worth noting that making a call doesn't require a SIM service. The Voice over Internet Protocol (VoIP) technology can make calls too, said Fong. With VoIP, scammers can fake phone numbers, making them difficult to trace, noted Fong.

There is mobile phone software available to block fraudulent calls, which users can download. That requires savvy users. Asking the government to force service providers to block suspicious calls is not the best approach, said Fong.

While many incoming calls from overseas prefixed "+852" are often high-risk fraud, there are also valid calls from Hong Kong residents abroad calling their Hong Kong offices or homes. Blocking all overseas "+852" calls may disable important time-sensitive calls, observed Fong.

SMS alerts

Since May 1, all mobile service providers in Hong Kong have been required by the Office of the Communications Authority to send voice or text alerts to customers advising them that an incoming call prefixed with "+852" is from outside Hong Kong. The free multilingual alerts aim to protect customers from scammers and fraudsters. But such calls will not be automatically blocked. In June, Under Secretary for Commerce and Economic Development Bernard Chan Pak-li announced that the SAR government would implement a registration system for corporate SMS users.

Organizations would be required to register before they could send SMS messages under their names. The banking sector will be the first to adopt this system, with a code of conduct expected to be issued and formally implemented by the end of the year, said Chan.

It can be challenging to trace scammers using fake social media accounts or fraudulent websites, as IP addresses can be easily changed with a Virtual Private Network (VPN), according to Fong.

Tech-savvy scammers

As technology evolves, high-tech fraud will become increasingly tricky, noted Yiu. Sophisticated AI scams are using fake IDs, face-swapping, and voice impersonation techniques. In April, a man surnamed Guo on the mainland was conned out of 4.3 million yuan ($600,000) by a scammer who stole the WeChat account of Guo's friend and impersonated him through AI face-swapping and voice-impersonation technology.

AI scams are easy to operate for those with advanced computer science skills, but challenging for the general public, especially the elderly, to understand and detect. Yiu added there is no effective way yet to combat AI scams, due to the rapid updates in technology.

In Fong's view, scamming techniques are introduced before anti-scamming measures are developed, in an unending cat-and-mouse chase. This creates an offensive and defensive play between scammers and police, with law enforcement often lagging the scammers.

Fong suggested the most effective way to combat fraud is through comprehensive anti-fraud education to increase public awareness and vigilance, to reduce the likelihood of individuals being scammed.

Low public awareness

The SAR government fraud prevention messages and techniques in recent years have not been sufficiently effective. A poll conducted by the Democratic Alliance for the Betterment and Progress of Hong Kong released in May showed that more than 50 percent of local residents were unaware of the "Anti-Scam Helpline 18222" — a service provided by the Anti-Deception Coordination Centre of the Hong Kong Police.

In addition, more than 70 percent of respondents were unaware how to use Scameter — a one-stop scam and pitfall search engine launched by the police. That is a depressing and dismal statistic on the effectiveness of law enforcement publicity.

Chow called for more effective methods such as using celebrities to sing catchy songs and announce easily remembered slogans, to imprint messages in the public mind.

For mainland students targeted by fraudsters, Chow recommended distributing leaflets when they collect their visas at the Immigration counters. She also proposed that the Immigration website can add a page alerting mainland students to this risk.

Yiu suggested the government use real-life examples instead of simply promoting slogans to alert the public. Creating short films would be an effective approach, said Yiu, in addition to fraud prevention education in primary and secondary schools, to raise awareness of scams from an early age.

Guard private data

Fong stressed the significance of protecting personal privacy to prevent fraud. He noted that personal information leaks are mostly caused by users themselves volunteering personal data, rather than leaks by communication service providers.

Social networking apps such as Facebook, Instagram, and LinkedIn include phone numbers, birth dates, email addresses, as well as education and work backgrounds. Users may give personal information when registering for online services, such as prize draws, websites, or online courses. Often, these services require such data before they allow access, as personal data is a vital currency in the digital economy.

Residents should limit the personal information they reveal, said Fong. He advised the public to regularly update the security and privacy of their personal accounts, improve the security levels of passwords for emails, social media, and payment tools, and added that it is prudent to install antivirus software on computers and mobile phones.

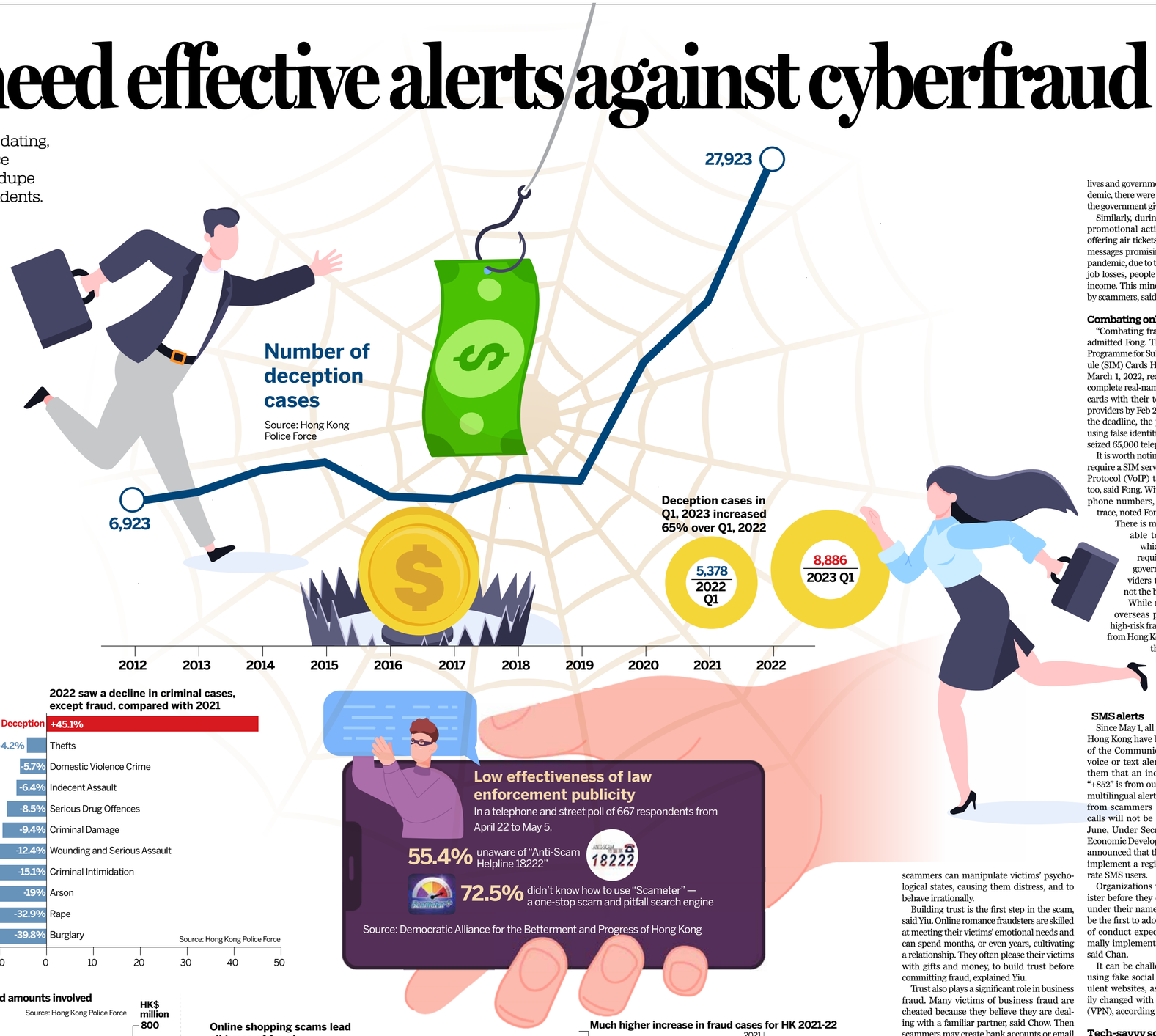
Don't shame victims

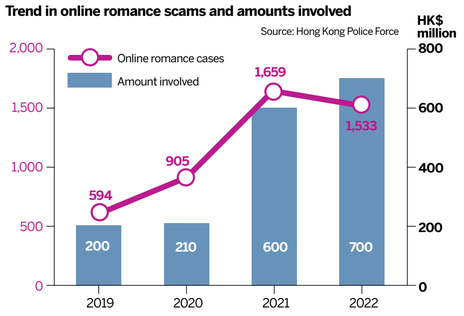
Vincent Cheng Shing, an assistant professor of Criminology and Social Policy Studies at Hong Kong Metropolitan University, suggested that in addition to promoting awareness of fraud prevention, the government should call for discretion not to condemn victims.

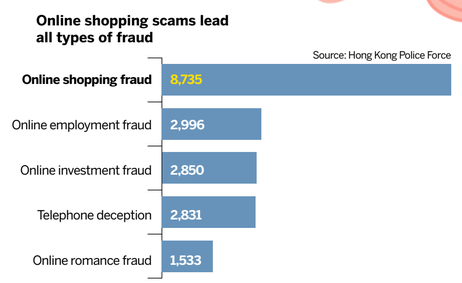
Condemning victims will discourage them from reporting the crime, making it even more challenging for law enforcement, said Cheng, noting that anyone can become a victim. He added that victim-blaming can further harm a traumatized individual already suffering psychological and material damage.

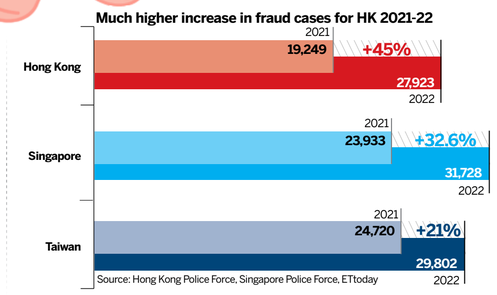
Until foolproof online fraud prevention can be devised, society has to be educated to be more alert, and to look out for itself.

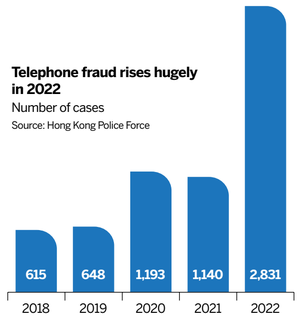
Contact the writer at oasishu@chinadailyhk.com











> "Free trade is a defining characteristic of Hong Kong as an international financial hub. If financial controls are too strict, it could dissuade businessmen from investing in the city, but if the controls are too lenient, it could pose risks. Combating scams in Hong Kong involves a balance between freedom and security."
>
> ***Bob Yan Xianming,*** *Hong Kong solicitor*

> "The so-called 'Hong Kong scam' does not only involve victims or perpetrators in Hong Kong but also other regions."
>
> ***Anita Chow Cheuk-ying,*** *fraud case litigator and partner at Morley Chow Seto*

> "Scamming techniques are introduced before anti-scamming techniques are developed, in an unending cat-and-mouse chase. This creates an offensive and defensive play between scammers and police, with law enforcement often lagging the scammers."
>
> ***Francis Fong Po-kiu,*** *honorary president, Hong Kong Information Technology Federation*

> "While most people are cautious when asked for personal information or money, scammers can manipulate victims' psychological states, causing them to become distressed, and to behave irrationally."
>
> ***Yiu Man-ho,*** *president, Global Anti Scam Association and private investigator*

WHAT'S NEXT

1. **Use celebrities for anti-fraud publicity instead of just slogans.**
2. **Target alerts to the elderly, women, mainland plus overseas students, and internet novices.**
3. **Limit volunteering personal info and strengthen passwords when using social media.**
4. **Do not blame fraud victims, support them.**

Infographics: Dong Kai, Mok Kwok-cheong

Data Journalism

Let the facts speak

Our data journalism reports map the options for the community to resolve its challenges with consensus.

We analyze data from governments, industries, corporations, scholars, think tanks and nongovernment organizations.

We integrate the insights and policy prescriptions from domain experts.