



香港城市大學
City University of Hong Kong

ITED20260467 | Media and Information Literacy

Social Engineering in Scams

Prof. Jiang Li Crystal

Associate Head & Associate Professor

Department of Media and Communication

CityUHK - China Unicom Joint Laboratory for Intelligent Scam Prevention

City University of Hong Kong

專業 創新 胸懷全球
Professional • Creative
For The World

The Problem with “I Am Too Smart to Be Scammed”

Three misconceptions:

“I am careful.”

“I can recognize
suspicious people.”

“I would never fall
for a scam.”

Scams do not necessarily exploit ignorance.

They exploit normal human psychology.

What Is Social Engineering (社會工程)?

- Mann (2008) defines social engineering as “to manipulate people, by deception into giving out information, or performing an action”
- Rather than exploiting technological vulnerabilities, it targets human psychology to persuade individuals to act against their own interests

The person becomes part of the attack pathway.

Believable identity

可信身份

Convincing situation

合理情境

Pressure to act

行動壓力

Common Forms of Social Engineering

Pretexting

虛假情境

Creates a believable scenario to obtain information or access.

建立可信的虛假情境，套取資料或權限。

Baiting

誘餌攻擊

Uses rewards or attractive offers to trigger risky action.

以優惠或獎賞誘受害者採取高風險行動。

Tailgating

尾隨闖入

Tricks staff to gain physical entry to restricted areas.

欺騙職員，跟隨進入受限制區域。

Quizzing

問卷套料

Uses fake surveys or quizzes to collect personal information.

利用假問卷或測驗套取個人資料。

Scareware

恐嚇軟件

Claims a device is infected to sell fake security software.

訛稱裝置中毒，推銷虛假防毒軟件。

Phishing

釣魚詐騙

Uses deceptive messages to steal data or deliver malware.

以欺詐訊息套取機密資料或散播惡意程式

Authority

權威施壓

Uses status or power to demand sensitive information.

利用權力或職位要求他人交出敏感資料

Dumpster Diving

翻找棄置資料

Collects information from documents that were not destroyed.

從未妥善銷毀的棄置文件收集資料。

Hoax

虛假騙局

Creates a deceptive claim to steal confidential information.

製造虛假騙局，竊取機密資料。

Vishing

電話詐騙

Impersonates a trusted person or institution by phone.

透過電話冒認可信人士或機構。

Whaling

高層獵捕

Targets senior executives with tailored deception.

以度身訂造的騙局針對機構高層。

Pharming

網站轉址

Redirects users to lookalike websites to steal data.

將使用者轉往仿冒網站竊取資料。

Role of Technology in Social Engineering

Table 1. Integrated scam typology: narrative manipulation vs. interface exploitation.

Scam category	Subcategory	Narrative hooks	Narrative/manipulative tactics	Technological enablers
Narrative-Driven Scam	Lure of Gain	Wealth	High return promises	Cryptocurrency, Trading bots
		Relationship	Romantic bonding, future planning	AI-driven conversational agents / Synthetic identity generation
	Fear of Loss	Opportunity	Elite jobs, scholarships, etc.	Web spoofing / Domain impersonation
		Safety	Police impersonation, fake arrests	Voice synthesis / Deepfake simulation
		Property	"Account freeze," "fund withdrawal" alerts	Message spoofing / Credential phishing systems
		Privacy	Blackmail, reputational damage framing	Identity cloning / Data aggregation tools
Interface-Manipulated	Misclick	—	Misleading buttons/pop-ups	Malicious UI injection / Overlay manipulation
	Misinput	—	Phishing pages, fake login flows	Phishing automation toolkits
	Misrecognition	—	Fake support search results	SEO poisoning / Service impersonation
	Mistrigger	—	System alert loops, countdowns	Script-based dialog loops / Browser hijack
	Remote Control	—	Fake tech support, remote install	Remote control protocols / Social engineering tools

Technology supplies credibility.

Social engineering converts credibility into action.

Social Engineering Goes Beyond Money



Fraud & Account Harm

- Financial scams
- Phishing
- Impersonation
- Gaming and virtual-item scams
- Fake jobs and opportunities
- Account takeover

金錢損失、帳戶被盜及資料外洩



Relationship & Image-Based Harm

- Online grooming
- Romance manipulation
- Sextortion
- Coercion to share private images
- Emotional control and isolation

心理困擾、性剝削及聲譽受損



Peer & School-Context Manipulation

- Fake teacher/classmate identities
 - Cyberbullying
 - Manipulation to share passwords, images or information
 - Requests to conceal communication from adults
- 信任受損、社交孤立及持續受害

上述操縱方式很多都涉及社會工程

**The target may be money, information, access, private images
or control over another person.**

Case Study: Deepfake Authority in Action



HK\$200M

lost after a fabricated video conference

一場偽造視像會議造成約二億港元損失

- 1 In late January 2024, an employee received a phishing email that appeared to come from the UK head office's Chief Financial Officer.
- 2 The employee joined a group video conference concerning alleged confidential transactions.
- 3 People resembling the Chief Financial Officer and other colleagues appeared in the meeting.
- 4 Following the instructions, the employee authorised transfers to five local bank accounts.

HOW PEOPLE ARE MANIPULATED

From trust cues to pressured action

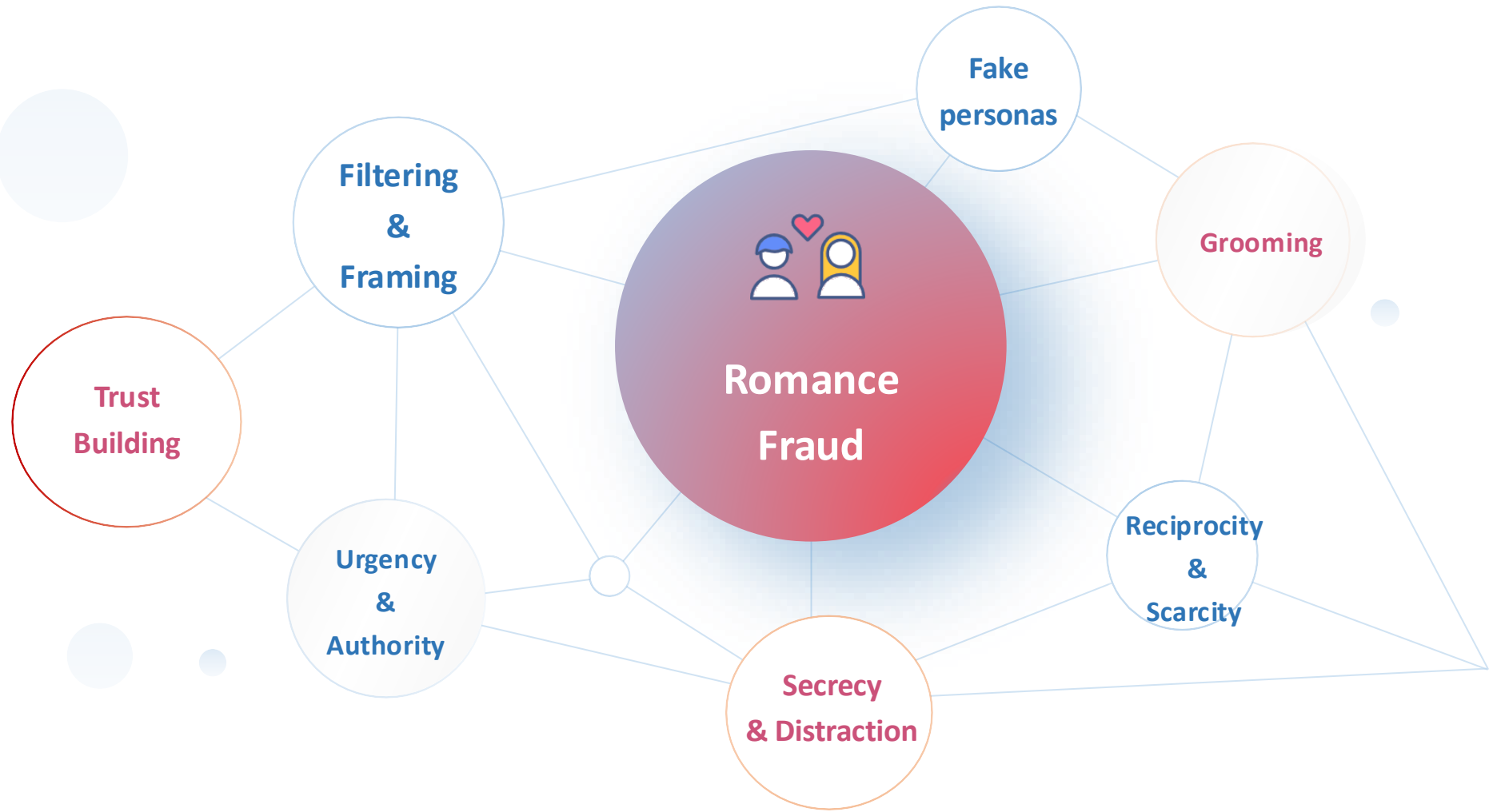
What makes a harmful request feel safe, urgent or difficult to refuse?

Different Scams, Different Vulnerabilities

SCAM TYPE	LIKELY TARGETS	CONDITIONS EXPLOITED
Impersonation	Adolescents	Lack of Experience · Overtrust
Account / Phishing	Students · Gamers	Fear · Urgency · Cognitive load
Romance / Grooming	Adolescents · Older adults	Attachment · Loneliness
Investment	Adults with savings	Financial anxiety · Expert signals
Job / Task	Students · Graduates	Opportunity · Urgency · Sunk cost
Shopping / Tickets	Students · Young consumers	Scarcity · Attractive offers
Fake Authority	New arrivals · Students	Institutional unfamiliarity · Fear

The same person can be resilient in one context and vulnerable in another.

Psychological Manipulation Tactics in Romance Fraud



Case Study: A Local Romance-Investment Scam

A 49-year-old landlady posted a flat for rent on Xiaohongshu. The “interested tenant” gradually became an online romantic partner—and then an investment adviser.

一名49歲女業主在小紅書放租；「租客」逐步變成網戀對象，再以投資專家身分誘導她入局。

1
Rental Enquiry

以租樓接觸

2
Familiar Chat

建立熟絡感

3
Romance

發展網戀

4
Investment Advice

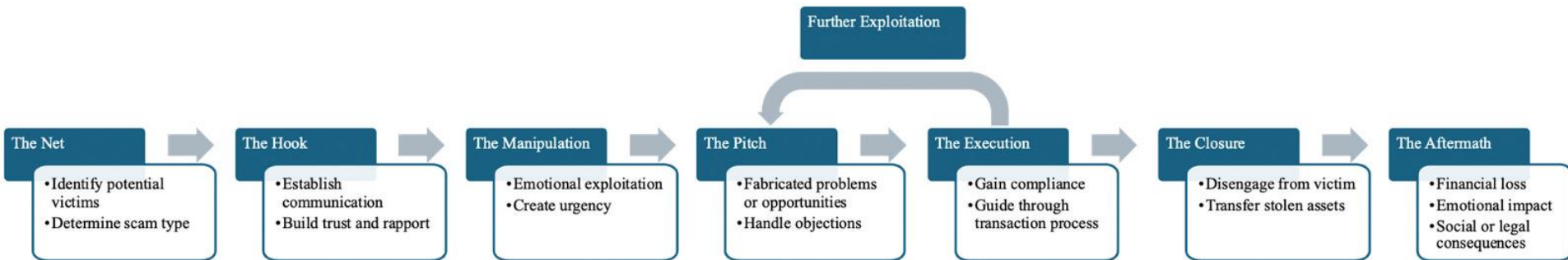
提供投資建議

5
HK\$2.5M Loss

損失252萬元

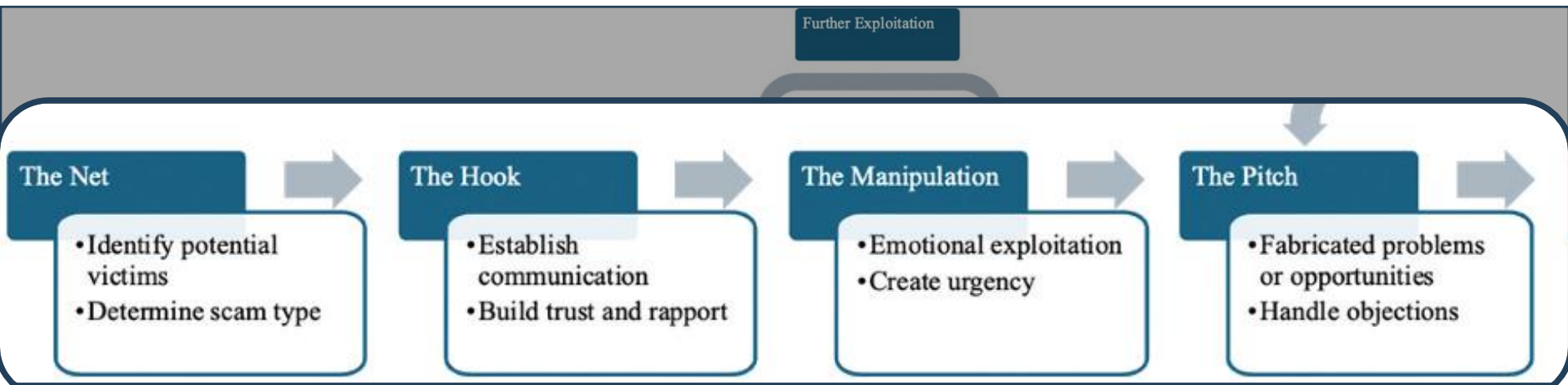


Multi-Stage Deception Tactics



Liu, X. F., Ai, Y., Jiang, L. C., Wang, X., & Wu, Y. (2024). Understanding the human element in scams: a multidisciplinary approach. *Journal of Information Technology Case and Application Research*, 1–16.
<https://doi.org/10.1080/15228053.2024.2439192>

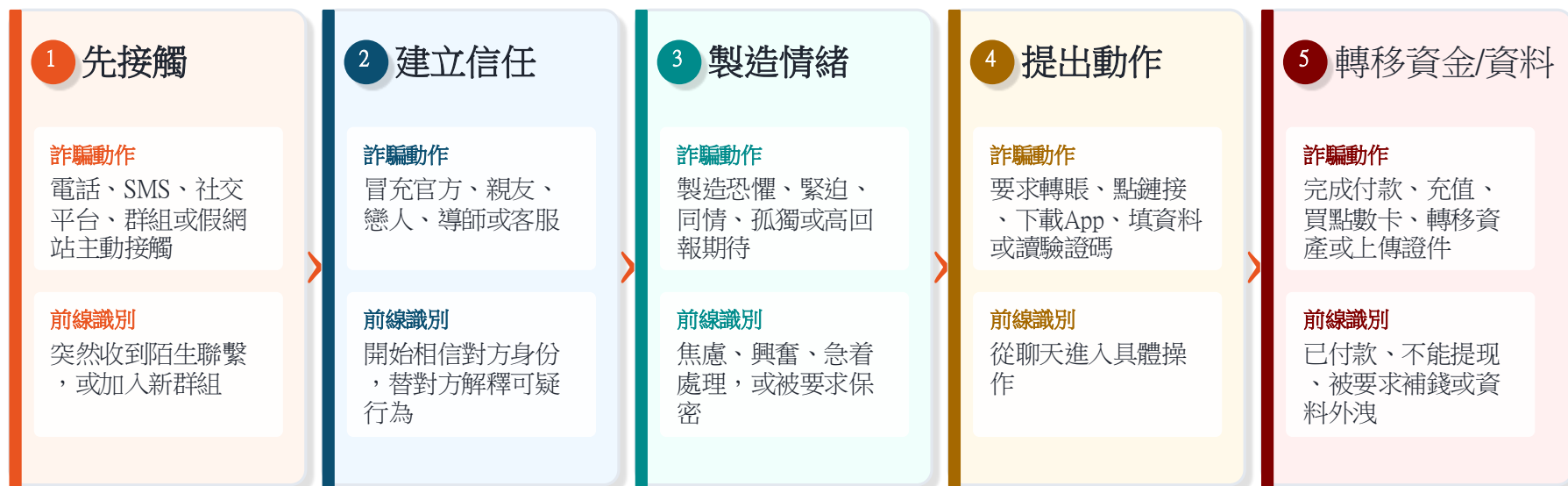
Multi-Stage Deception Tactics



Liu, X. F., Ai, Y., Jiang, L. C., Wang, X., & Wu, Y. (2024). Understanding the human element in scams: a multidisciplinary approach. *Journal of Information Technology Case and Application Research*, 1–16.
<https://doi.org/10.1080/15228053.2024.2439192>

Different Scams, Similar Process

不同詐騙，底層流程相似



電話、情緣、投資、假官方，底層都是推進式操控。

The Language of Manipulation

Fake Persona

假身份

"I'm from your school / the police."

Trust Building

建立信任

"You can rely on me."

Reciprocity

互惠

"I helped you—can you help me?"

Scarcity

稀缺

"Only two places left."

Urgency

緊迫

"You have ten minutes."

Secrecy

保密

"Do not tell your parents."

Authority

權威

"This is an official investigation."

Emotion Hijacking

情緒劫持

Fear · attachment · excitement · anger

We are not as good at detecting deception as we think we are

- Human beings are only **54%** accuracy rate in deception research (Bond & DePaulo, 2006)
- Alternative approaches are **also ineffective** :
 - **Cognitive approach** to lie detection only associated with a small effect (Levine et al., 2017)
 - **AI** personas yielded varying results (both truth biased and lie-biased; Markowitz & Levine, 2025)



Psychological Basis of Susceptibility

Truth Bias

People assume
honesty by default
(evolutionarily
adaptive)

Cognitive Load

Fast decisions
under uncertainty

Affective Forecasting Errors

Misjudging future
regret/hope

When Students May Be More Vulnerable

New Environment

Unfamiliarity with local institutions, procedures and trusted support channels.

不熟悉本地機構、程序及可信求助渠道。

Expanding Independence

Students may handle money, accounts and major decisions independently for the first time.

學生可能首次獨立處理金錢、帳戶及重要決定。

Need for Belonging

Friendship, romance and peer approval can be used to build trust or pressure compliance.

詐騙者可利用友誼、感情及朋輩認同建立信任或施壓。

Financial and Career Pressure

Scholarships, part-time jobs, investments and “easy money” offers may appear especially attractive.

獎學金、兼職、投資及輕鬆賺錢的機會可能格外吸引。

Barriers to Seeking Help

Fear of embarrassment, punishment or worrying family members may delay disclosure.

害怕尷尬、受責備或令家人擔心，可能導致延遲求助。

Vulnerability is situational—not a label attached to students.

Case Study: Fake Uniform. Fake Police. Real Loss.

假公安主動來電

一名21歲女大學生接到自稱內地公安的來電，被指涉及金融犯罪。

以刑責及牽連家人製造恐懼

騙徒聲稱一旦洩密，女生及父母都可能面臨刑責，令她不敢向外求助。

操控女生自拍“被綁架”影像

騙徒要求制作假伤势及被捆绑影像，再向其父母勒索300万港元。女生父亲察觉有异并报警，香港警方联络泰国警方后寻回。

利用制服與文件建立權威

騙徒在視像通話中展示公安制服及徽章，要求女生簽署保密協議並接受實時監控。

要求轉帳及離港配合調查

女生按指示以升學為由向家人取款，父親轉帳**140萬港元**；其後她再被要求獨自前往泰國。

Case Study: From an Online Friend Request to HK\$70,000 Sextortion

主動接觸

一名17歲男學生在Telegram收到交友邀請，對方假扮成高顏值女網友。

資料外洩

學生透過連結下載不明軟件，導致手機通訊錄外洩。

威脅及付款

騙徒威脅將影片發送給其親友。學生在一日內三次轉帳，損失逾7萬港元，其後報案。



引起好奇

對方傳送一條連結，聲稱內有自己的私人相簿。

誘導越界

騙徒誘使學生進行私密視像通話，並暗中錄影。

本土數據：

兩星期內接近60宗個案 | 損失逾240萬港元 | 超過四成受害人為學生

數據來自：香港警方2025年7月16日至30日期間接獲的裸聊勒索案件

Case Study: From an Instagram “New Friend” to a HK\$5,000 Loss

01 主動接觸

一名13歲中二男生在Instagram認識了一名新朋友。

03 製造期待

約一星期後，這名朋友相約學生在旺角見面。

05 騙取金錢

學生透過支付寶分三次轉帳至兩個本地轉數快戶口。

02 轉移平台

雙方其後轉到WhatsApp繼續私人聊天。

04 加入付款條件

對方要求學生在見面前繳付5,000港元保證金。

06 加碼並失去聯絡

對方沒有現身，反而要求更多。學生因餘額不足向父親求助，才發現受騙並報警。

本土數據：

半年超80宗個案 | 損失逾370萬港元 | 近兩成受害人為20歲以下青少年

數據來自：香港警方2025年警方網罪科於社交平台Facebook專頁CyberDefender 守網者

Young Jobseekers: Fake Orders and Part-time

在家輕鬆賺錢

機制 用低門檻、高回報吸引求職青年

信號 只強調快賺錢，工作內容模糊

先墊付後返傭

機制 先付款完成任務，再承諾返本金與佣金

信號 求職變成用自己的錢下單或充值

任務越多佣金越高

機制 用升級任務引導投入更多資金

信號 金額逐步增加，要求做完下一單才可提款

先刷流水

機制 以平台信用、流水或激活佣金為由要求轉帳

信號 資金操作被包裝成正常流程

先交培訓費 / 保證金

機制 以入職、培訓、設備或開戶為由先收費

信號 未入職已要求付款，且公司資料難以核實

刷單兼職的核心風險：把找工作變成先付款，再用任務升級持續加碼。

Case Study: Fake Internship, Real Loss

招聘接觸

一名19歲大學一年級學生透過LinkedIn申請實習職位。

建立可信度

騙徒以流利英語溝通，詳細介紹公司背景，並安排40分鐘網上培訓。

加碼與損失

任務要求她投入愈來愈多資金，最終損失接近港幣19萬元。

轉介工作

自稱「人事公司」的機構表示原職位已滿，轉而推薦一份在家完成的兼職。

小額回報

她在所謂公司網站完成「購買產品」任務，期間三次收到佣金，最高一次達港幣7,000元。

1

Recruitment

招聘接觸

2

Redirection

轉介新職位

3

Professional Setup

專業包裝

4

Early Rewards

初期回報

5

Escalation

加碼損失

<https://www.adcc.gov.hk/zh-hk/alerts.html>

Case Study: HK\$100 an Hour, HK\$4 Million in Debt

招聘接觸

一名30歲女售貨員在香港求職平台刊登履歷，其後透過WhatsApp收到工作邀請。

建立僱傭關係

日常文書工作令她相信自己已正式受聘。

持續加碼

她先後申請多筆貸款，並向指定銀行戶口轉帳**超過港幣400萬元**，最終未能取回款項。

時薪 100 元

背400萬債？

返新工，千祈咪幫

公司貸款周轉！

即睇騙徒4大藉口



正常工作包裝

她獲聘為在家工作的行政助理，時薪為港幣100元。

工作包括整理表格，以及比較官方網站與二手平台的手錶價格。

代公司借貸

約兩個月後，「僱主」要求她以個人名義申請貸款，聲稱用作公司周轉，並承諾全數歸還。

Children and the Young: Gaming, Social Media and Sextortion

遊戲內私聊

風險：陌生人透過好友、戰隊、語音房接觸，逐步轉到其他平臺私聊。

信號：避開家長聊天、突然更換平臺，不願說明對方身份。

假充值 / 虛擬物品交易

風險：以低價皮膚、遊戲幣、裝備或代充值為誘餌，要求先付款。

信號：突然要錢、買點卡、提供驗證碼，或帳號異常登入。

帳號盜用

風險：誘導點擊假登入頁、分享驗證碼、綁定陌生郵箱或手機。

信號：帳號無法登入、資料被改，好友收到異常訊息。

陌生人誘導

風險：以交友、送禮、粉絲福利、陪玩或任務挑戰建立信任。

信號：開始保密、收禮，按要求拍照、轉帳或完成任務。

私密影像勒索

風險：誘導發送私密照片、視頻或裸聊，再威脅公開勒索。

信號：突然焦慮、害怕手機被看，情緒低落或提到被威脅。

害怕被責罵而沉默

風險：擔心被責備、沒收手機、被學校知道，因此不敢求助。

信號：刪除聊天記錄、回避溝通、突然要錢或失眠。

先確保安全，再處理責任；
讓孩子知道說出來不會先被罵，比單純禁止上網更重要。

Case Study: One Code, Multiple Victims

Tony received a WhatsApp message from a friend asking for a six-digit verification code. After he shared it, his account was taken over.

Tony收到朋友的WhatsApp訊息，要求提供六位數驗證碼；分享後，他的帳戶隨即被騎劫。

1

Trusted Contact

熟人訊息

2

Small Request

簡單要求

3

Account Takeover

帳戶被騎劫

4

Impersonation

騙徒冒認Tony

5

Point-card Loss

遊戲點卡損失

OUR RESPONSE CAN CHANGE WHAT HAPPENS NEXT

From blame to safety

Stop the harm. Preserve the evidence. Keep the student connected to support.

The First Five Minutes After Disclosure

1

Stabilise

穩定情緒

“Thank you for telling me. You did the right thing.”

Stay calm and listen without blame.

2

Stop Further Harm

阻止損失擴大

“Do not reply, pay or follow further instructions.”

Pause contact and transactions.

3

Preserve Evidence

保留證據

“Keep the messages. We may need them later.”

Save screenshots, usernames, links and records.

4

Connect Support

連接支援

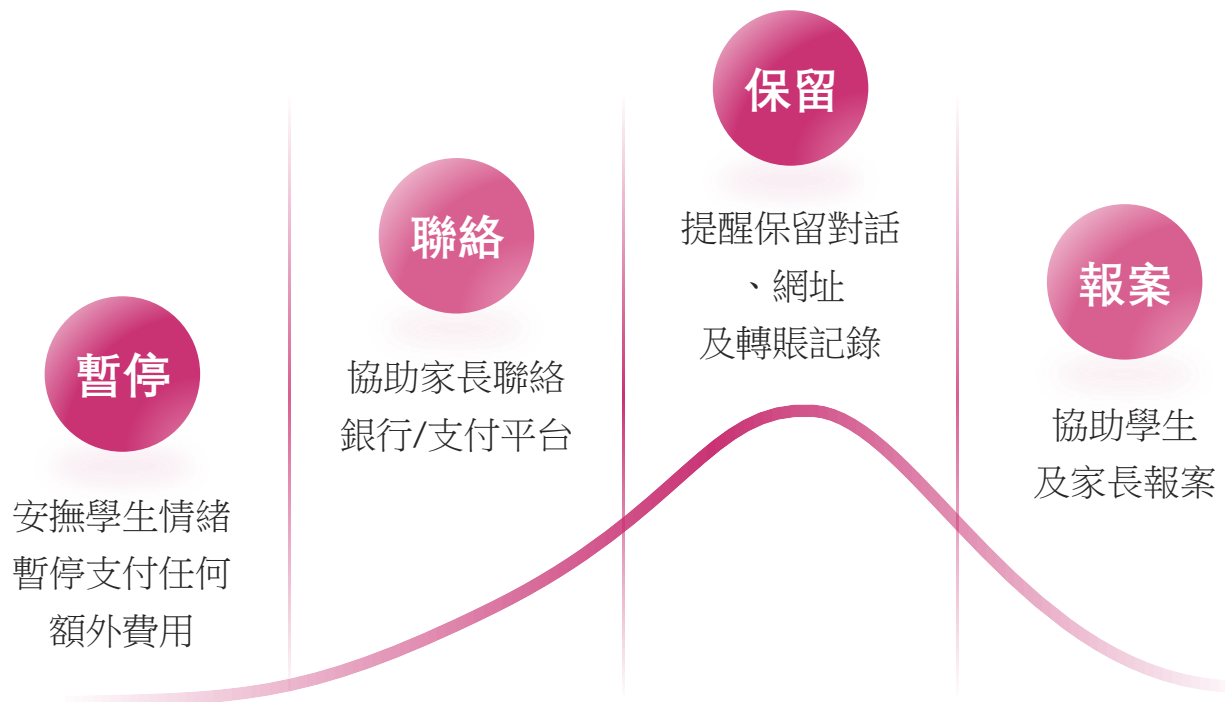
“You do not have to handle this alone.”

Follow safeguarding procedures and seek support.

Case Study: Game Account Trading

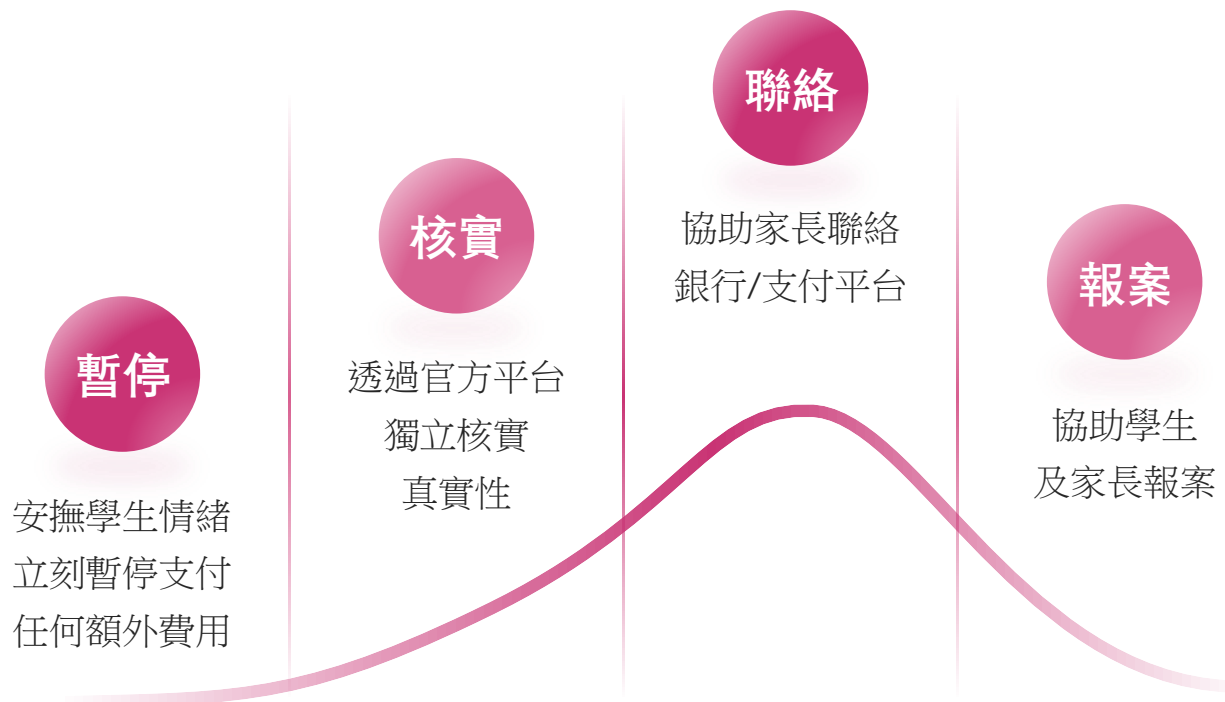
2024年9月，警方公布一星期內接獲14宗遊戲帳戶買賣騙案，8名受害人為學生，最年幼受害人**12歲**，全部案件合共損失約27萬元。

騙徒以高價收購帳戶作招徠，再引導受害人進入假交易平台，聲稱提款須先繳付保證金。



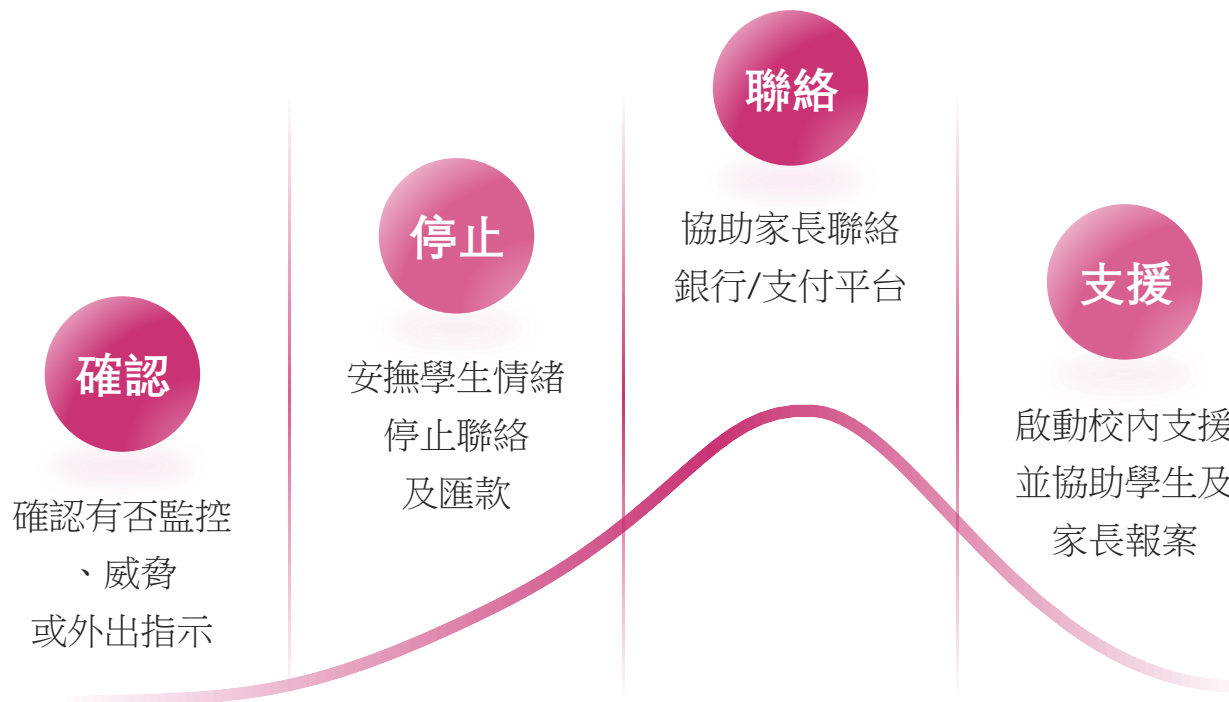
Case Study: Concert Ticket Scam

2026年1月18日，TVB東張西望節目報道，一名女中學生在二手平台購買兩張BLACKPINK演唱會門票，原價合共7,000港元。賣家以付款狀態及系統問題為藉口，要求追加付款，累計轉帳金額為**12,500港元**。其母其後向支付平台查詢並報警。



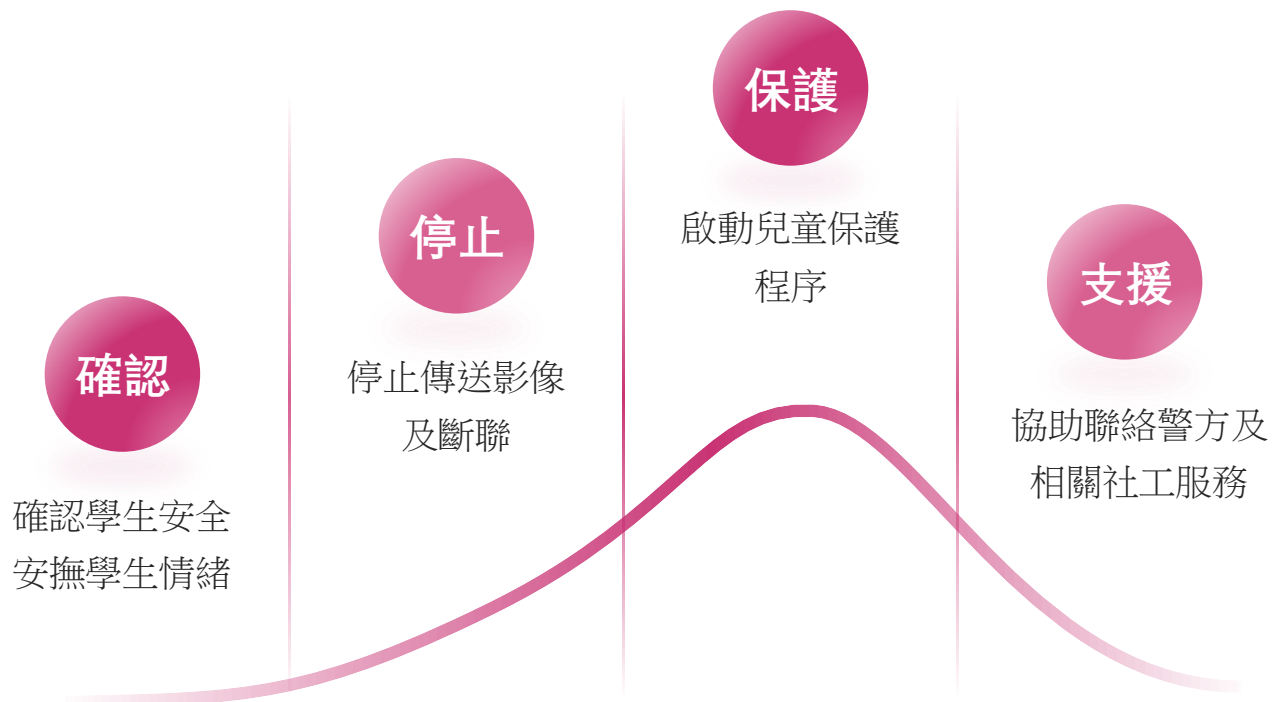
Case Study: Fake Police Call

2022年6月13日，東網報道警方公布的案件：一名14歲女中學生接獲假速遞職員來電，其後轉接至假公安，被指涉及洗黑錢。騙徒要求她交出母親的身份證相片、銀行資料及密碼，並指示她登入母親的網上銀行匯款。母親其後發現約**80萬港元**損失。

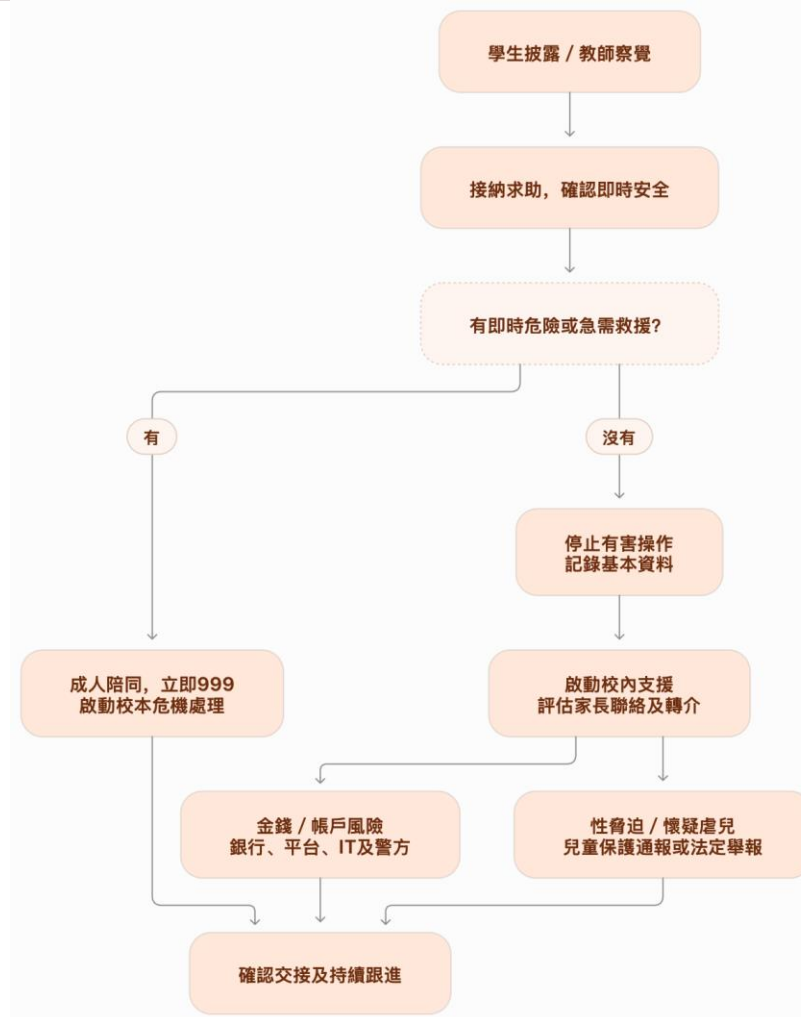


Case Study: Online Sexual Coercion

2024年10月12日，警方在教育界反詐騙活動中披露，一名11歲女小學生在網上遊戲平台認識網友，對方誘使她進行裸聊，再威脅她提供更多裸照，最終由父親報案。



School Response to a Student Scam Disclosure



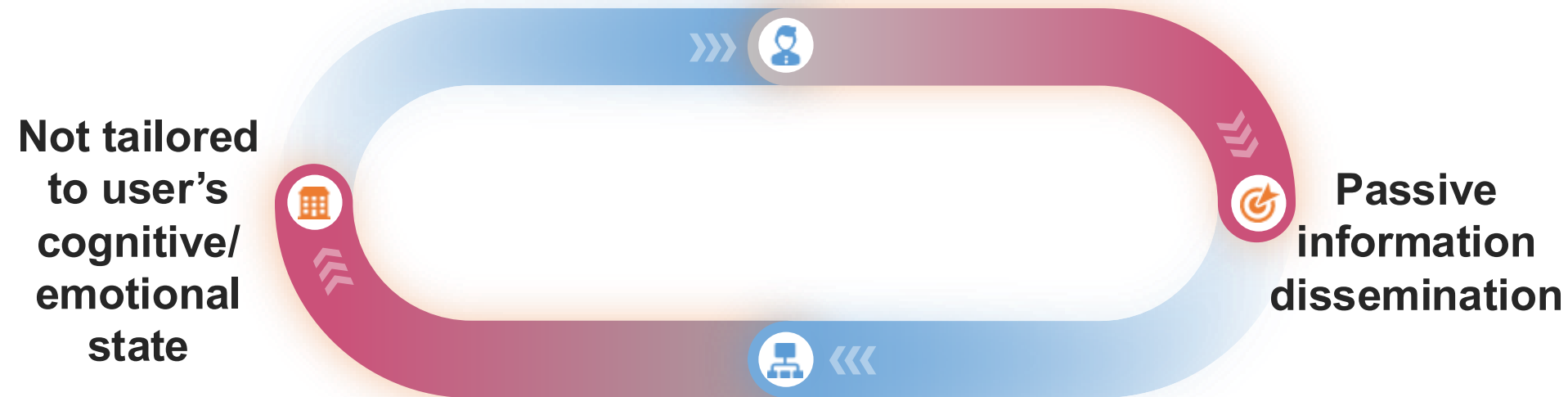
WHY “JUST BE CAREFUL” Is Not Enough

Students need recognisable warning signs, rehearsed actions and a safe route to help.

學生需要可辨識的警號、練習過的行動，以及安全的求助途徑。

Current Anti-Scam Communication: Limitations

Static Awareness Campaigns



Over-saturation of warnings → psychological reactance

Challenges to Current Anti-Scam Communication

Repetition

The same slogans appear again and again, so people gradually stop noticing them.

Complexity

Long lists of scam types are difficult to remember under pressure.

Competition

Warnings compete with messages, advertisements and app notifications.

Low Personal Relevance

Generic examples can make students think, “This would never happen to me.”



Effective warnings should make the next safe action clear.

Awareness Is Not the Same as Protection

WHAT THE STUDENT KNOWS

“I should not click suspicious links.”

“我不應點擊可疑連結。”

≠

WHAT THE STUDENT RECEIVES

“Your school account will be suspended in 10 minutes.”

“你的學校帳戶將於10分鐘後被停用。”

AUTHORITY · URGENCY · FEAR · COGNITIVE LOAD

Knowing the rules ≠ following the rules

Protection requires a response that students have already practised.

Practical Actions for Students



Spot urgency,
authority, secrecy or
unrealistic rewards.

留意催促、權威、保
密要求或不合理回報



Do not click, reply,
pay or share codes.

不要點擊、回覆、
付款或分享驗證碼



Check through
an official channel
you find yourself.

自行查找
官方渠道核實



Save the evidence
and tell
a trusted adult.

保存證據，盡快向可
信成人求助。

RECOGNISE

辨識

PAUSE

暫停

VERIFY

核實

TELL

求助

A School-Based Anti-Scam Education Model

REAL SCENARIO

真實情境展示

Use a real case such as fake school or teacher message as the case.

PRACTISE THE RESPONSE

情境演練

*Apply
Recognise, Pause,
Verify and Tell.*

SCHOOL SUPPORT

校內求助途徑

Display the school's official contact route: teachers, school officers or social workers.

REGULAR REVIEW

定期鞏固

Use short monthly scenarios, parent reminders and a Scameter+ demonstration.

LEARNING CHECK

Before leaving, each student identifies **one warning sign, one official verification channel and one trusted adult at school.**

Conclusion & Key Takeaway

UNDERSTAND

理解人性

*Scams exploit
trust and pressure.*

RECOGNISE

辨識操控

*Look for the pattern,
not only
the scam type.*

PRACTISE

練習應對

*Recognise - Pause
- Verify - Tell*

SUPPORT

支持求助

*Preserve evidence
and respond
without blame.*

Help students pause, verify and speak up early.