ProtectMyDataSolutions / Scam-Safety

THE 2026 EDITION · EDITION 1

The 2026 Scam-Safety Report

What the official data says about scams and phishing worldwide, and the simple habits that stop them. A guide for families, schools and anyone who has ever asked who is really calling.

PUBLISHED	COVERAGE	EDITION	BY
November 2026	Global · Asia focus	First edition	ProtectMyDataSolutions

Compiled from official government, law-enforcement and recognised anti-scam sources, each cited in full on the final page. Figures reflect reported data only, so true totals are higher. This guide is general safety information, not legal or financial advice.

EXECUTIVE SUMMARY

01 Five things to know

Scams are rising in value even where the number of reports is flat or falling. The pattern behind almost all of them is the same: convince you to trust the wrong sender, then make you act before you think. Here is what the official data shows.

1

US$20.9 billion

reported lost to online crime in the United States in 2025, up 26% on 2024, across more than one million complaints for the first time.

FBI IC3, 2025 Internet Crime Report (April 2026).

2

Losses up, reports flat

US reported losses rose from US$4.2bn in 2020 to US$20.9bn in 2025 while complaint numbers barely moved. Each victim is losing far more.

FBI IC3 annual reports, 2020 to 2025.

3

57% of adults

worldwide said they had met a scam in the past year, and 23% of those scammed lost money, across 46,000 adults in 42 countries.

GASA and Feedzai, Global State of Scams 2025.

4

Phishing comes first

Phishing is the most common first step in a scam: about 60% of intrusions in the EU begin there, and 3.8 million phishing attacks were observed in 2025.

ENISA Threat Landscape 2025; APWG, 2025.

5

Asia is a front line, and awareness works

Singapore lost over S$1.1 billion to scams in 2024; Japan, Hong Kong and South Korea all set records. Yet Australia cut reported losses by almost 26% in one year through coordinated action. The curve can be turned, and habits are a large part of how.

Singapore Police Force 2024; Japan NPA 2024; Hong Kong Police 2024; South Korea NPA 2024; Australia National Anti-Scam Centre 2024.

WHAT IS INSIDE

02 Five things to know
03 The global landscape
04 Where the money goes
05 The first contact: phishing
06 Asia in focus
07 How modern scams work
08 The 12-point checklist
09 For schools
10 Where to report
11 Methodology and sources

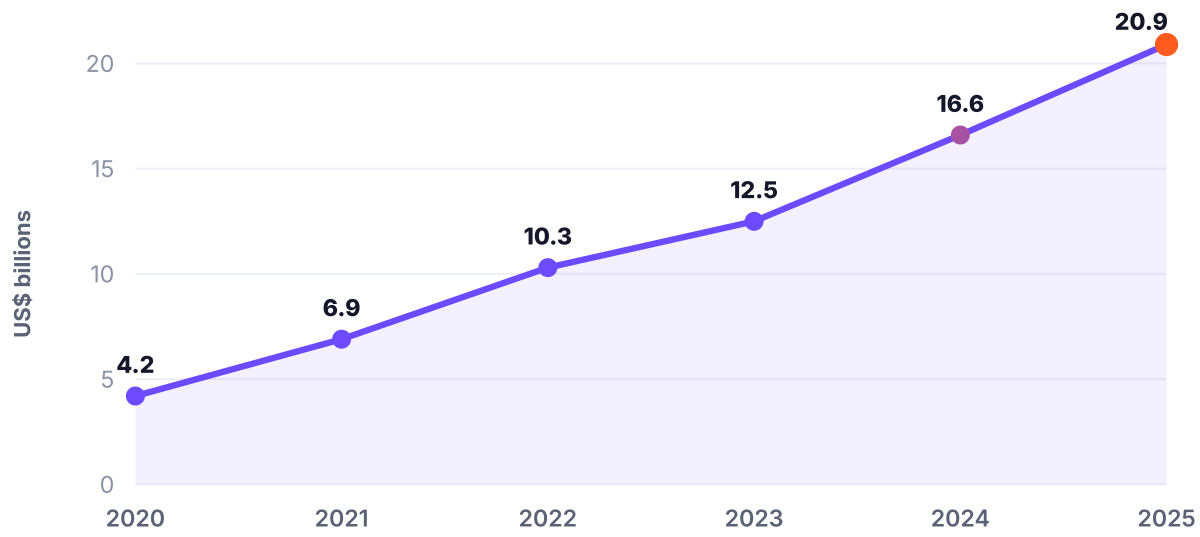
THE GLOBAL LANDSCAPE

02 A rising cost, not more reports

Across the biggest official datasets the same shape appears: the money lost keeps climbing even as the number of reports holds steady or falls. Scams are getting more effective per attempt, not simply more numerous. The chart below uses the longest consistent public series, the FBI's annual Internet Crime Report.

Reported online-crime losses, United States, 2020 to 2025

US dollars, billions. Reported losses more than doubled in two years and have grown every single year.



Source: FBI Internet Crime Complaint Center (IC3), annual Internet Crime Reports 2020 to 2025 (2025 report released April 2026). Figures are reported losses only.

GLOBAL · US

1,008,597

complaints filed with the FBI's IC3 in 2025, the first year ever above one million. Investment fraud was the largest loss category at US$8.6bn, more than 40% of the total.

FBI IC3, 2025 Internet Crime Report (2026).

GLOBAL

US$442 billion

estimated lost to scams worldwide in the past year, based on a survey of 46,000 adults across 42 countries. 57% had encountered a scam; shopping scams were the most common type.

GASA and Feedzai, Global State of Scams 2025 (October 2025).

US CONSUMER

US$12.5 billion

reported lost to fraud by US consumers in 2024, up 25%. The share of people who reported a fraud and lost money rose from 27% to 38% in one year.

US Federal Trade Commission (FTC), March 2025.

UK

£2.3 billion

reported lost to fraud in the UK in 2024 across 318,848 reports. Online shopping and auction fraud was the most reported category.

UK Action Fraud, 2024 data (reported 2025).

Reported figures are a floor, not a ceiling: many victims never report, so the real totals are higher. We cite them to show scale and direction, not to alarm.

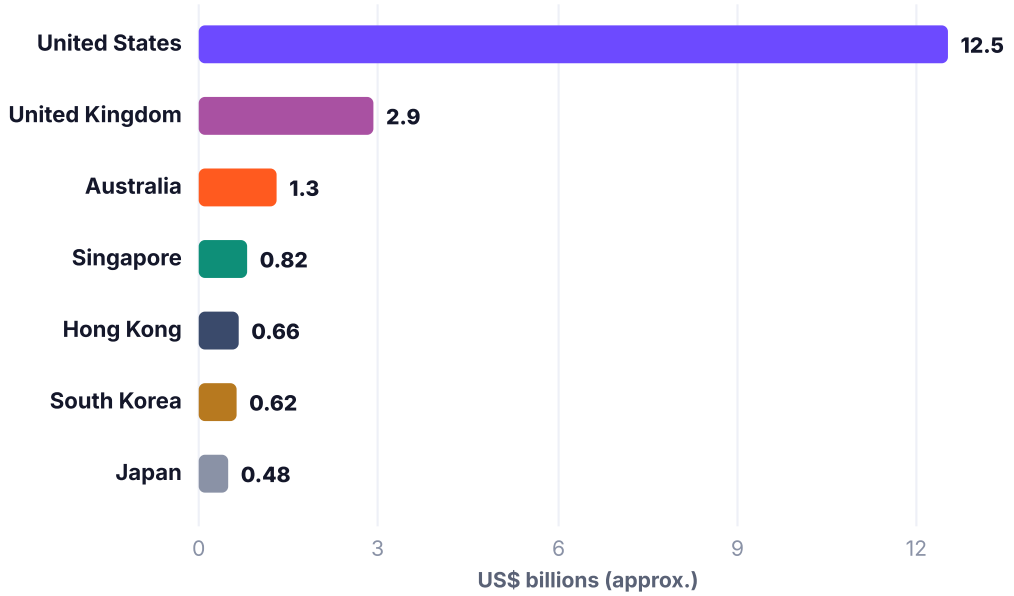
THE GLOBAL LANDSCAPE

03 Where the money goes

Two questions matter for a family or a school: where in the world are losses heaviest, and what kinds of scam take the most money. The two charts below answer each in turn, from official national and regulator data.

Reported scam and fraud losses, latest full year, selected markets

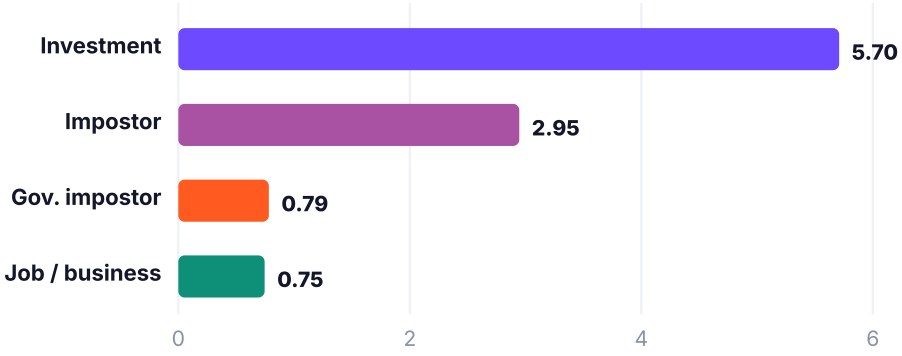
Converted to US dollars for scale only. Definitions and scope differ by country, so read this as relative size, not a strict ranking.



Sources: US FTC 2024 (consumer fraud, US$12.5bn); UK Action Fraud 2024 (£2.26bn); Australia NASC 2024 (A$2.03bn); Singapore Police Force 2024 (S$1.11bn); Hong Kong Police 2024 (technology crime, HK$5.13bn); South Korea NPA 2024 (voice phishing, KRW 854.5bn); Japan NPA 2024 ("special fraud", ¥71.9bn). Converted at approximate late-2026 rates.

US consumer fraud losses by category, 2024

Investment scams take the most money; impostor scams are the most frequently reported. US dollars, billions.



Source: US Federal Trade Commission, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 2025). Impostor scams were the most reported category by volume.

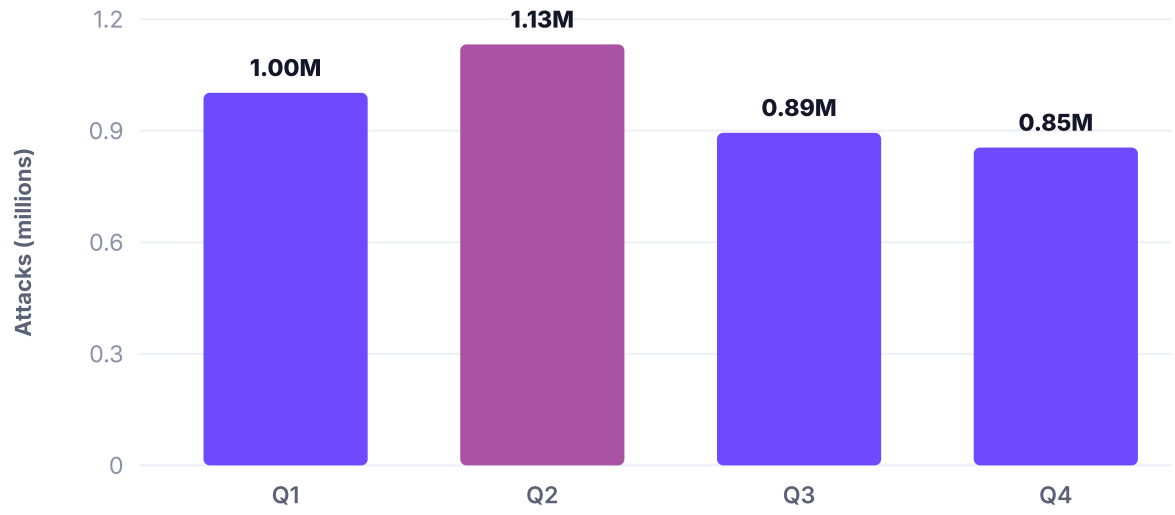
THE FIRST CONTACT

04 Phishing is how it starts

Behind most scams and most breaches is a single first move: a message built to look like it came from someone you trust. Email, text, chat, a QR code on a poster. In the European Union's threat data, phishing is now the way in for around six of every ten intrusions, ahead of every technical exploit.

Phishing attacks observed worldwide, by quarter, 2025

Number of unique phishing attacks recorded each quarter. 3.8 million were observed across the full year.



Source: Anti-Phishing Working Group (APWG), Phishing Activity Trends Reports Q1 to Q4 2025. Q2 2025 was the largest quarterly total since mid-2023.

EU

About 60%

of intrusions in the EU begin with phishing, vishing or related social engineering, ahead of exploiting software flaws (21%). Based on 4,875 incidents analysed.

ENISA Threat Landscape 2025 (covers July 2024 to June 2025).

GLOBAL · US

Most reported

Phishing and spoofing is consistently the single most reported cyber-crime type to the FBI's IC3, drawing more complaints than any other category.

FBI IC3, 2024 Internet Crime Report.

The method keeps shifting. QR-code phishing ("quishing") on posters, parking meters and fake invoices is rising, because a printed code hides where it really leads. SMS phishing ("smishing") about parcels, tolls and tax is now one of the most common forms of all. The defence does not change with the trick: confirm the sender on a channel you already trust before you act. The checklist on page 8 turns that into a habit.

REGIONAL DEEP-DIVE

05 Asia in focus

Scams hit the Asia-Pacific hard, and the official numbers set records across the region in 2024. We highlight Asia because it is where ProtectMyDataSolutions runs its free Protected School program, and because the trends here show up elsewhere soon after.

SINGAPORE

S$1.1 billion

lost to scams in 2024, up 70.6%, across 51,501 scam cases. In the majority of cases, victims were manipulated into transferring the money themselves.

Singapore Police Force, Annual Scams and Cybercrime Brief 2024 (Feb 2025).

JAPAN

¥126.8 billion

lost to social-media-based investment and romance scams in 2024, a record. Separately, phone-based "special fraud" losses hit a record ¥71.9bn, with about 80% of victims first contacted by phone.

Japan National Police Agency, 2024 figures.

HONG KONG

HK$5.13 billion

lost to technology crime in 2024 across 33,903 cases. A rise in deception was the main driver of Hong Kong's overall crime figure for the year.

Hong Kong Police Force, 2024 crime figures.

SOUTH KOREA

KRW 854.5bn

(about US$0.6bn) lost to voice phishing in 2024, nearly double the 2023 figure. Scams impersonating institutions and officials drove much of the rise.

South Korea National Police Agency data, 2024.

THE CURVE CAN BE TURNED

Australia is the counter-example and the reason for optimism. Reported scam losses fell by almost 26% in 2024, to about A$2.03 billion, the first fall in years, after coordinated action by government, banks and telecoms and a sustained public-awareness push. Reports fell 17.8% as well. Awareness and simple habits move the number.

Source: Australia National Anti-Scam Centre, Targeting Scams 2024.

WHY THIS MATTERS FOR SCHOOLS

Schools carry parents' trust and children's data, which makes a school's name a valuable thing for a scammer to fake. A message that appears to come from the school, asking a parent to pay a fee or confirm details, is a classic impostor scam. Keeping school communication private and verifiable removes the easiest opening. The Protected School program, free for schools, is on page 9.

THE MECHANICS

06 How modern scams work

However convincing a scam looks, it almost always relies on the same handful of moves. Learn the moves and the disguise stops mattering.

1 **The fake sender**
An email shows a familiar name and logo, but the real address behind it is wrong by a letter or a whole domain. A display name is trivial to fake; the actual address and the links are where the truth is.

2 **The fake caller**
A call or text appears to come from your bank, a courier, the police or a government office. Numbers and caller names can be spoofed, so a familiar number on screen is not proof of who is really on the line.

3 **Urgency and payment pressure**
"Act now or your account closes." "Move your money to a safe account." "Pay with a gift card or crypto." The rush is the scam. Real organisations give you time and never demand those payment methods.

4 **The fake meeting or link**
An unexpected meeting invite or "document to review" leads to a login page built to steal your password. Treat unexpected invites, links and QR codes the way you treat unexpected callers.

5 **Business email compromise (BEC)**
A message, seemingly from a boss, a supplier or a lawyer, asks staff to change payment details or approve an urgent transfer. BEC quietly moves some of the largest sums of any scam type, one invoice at a time.

6 **Cloned voices and faces**
A short audio or video clip is now enough to mimic a familiar voice or face in a "family emergency" call or a fake video meeting. The context is engineered to feel real; the request for money or secrecy is the tell.

REAL CASE · FAKE VIDEO MEETING

In early 2024, a finance employee at the engineering firm Arup in Hong Kong joined a video call with people who looked and sounded like the company's chief financial officer and colleagues. Every other participant was an AI recreation. Following their instructions, the employee made 15 transfers totalling about HK$200 million (around US$25 million). The fraud came to light only after a later check with head office.

Source: Hong Kong Police and Arup's own confirmation, as reported by SCMP, CNN and the Financial Times, 2024.

REAL CASE · CLONED VOICE

Police and consumer agencies warn of "family emergency" calls where a cloned voice of a relative begs for urgent money. The advice is simple and low-tech: agree a private family "safe word", and if a caller cannot give it, hang up and call the person back on a number you already have.

Source: FBI public service announcement (Dec 2024) and FTC consumer alerts.

THE CORE ELEMENT

07 The 12-point checklist

Print this page, or keep it on your phone and share it with your family and your school group. If a message or call fails even one of these, stop and check before you act. One action per line.

01 **Check the real email address**, not just the display name.

02 **If a message pushes you to act fast, slow down.** Urgency is the tell.

03 **Call back on a number you already have**, never the one in the message.

04 **Confirm any money or data request** on a second, separate channel.

05 **Never share one-time passcodes** or login codes with anyone, ever.

06 **Treat gift-card, crypto or "safe account" requests** as scams.

07 **Check where a link really goes** before you tap; if unsure, type the address yourself.

08 **Verify who is really contacting you.** A familiar name or logo is not proof.

09 **Use an encrypted channel** for anything sensitive or private.

10 **Be wary of unexpected attachments and QR codes**, even from known names.

11 **Agree a private family "safe word"** for any emergency money request.

12 **If something feels off, check with someone you trust** before you act.

No single habit stops every scam, and no tool can keep anyone completely safe. But together these twelve remove the openings that almost every scam depends on: a trusted-looking sender and a reason to hurry.

WHY IT WORKS

Slow down

Nearly every scam needs you to act before you think. Pausing to verify on a second channel defeats the single tactic they all share.

SHARE IT

Teach one person

Scammers target the least-prepared member of a family or team. Passing this list to one more person closes the easiest door.

ANNEX · EDUCATION

08 For schools

A school is a trusted sender to hundreds of families and a keeper of children's data, which is exactly what makes it worth impersonating. The good news is that a school can close the easiest openings with a few practical steps, and keep its everyday communication both private and verifiable.

FREE FOR SCHOOLS

The Protected School program

Through the Protected School program, free for schools, a school can keep its communication with staff, parents and students private and verified:

- Encrypted email and calls, so only the school and its community can read them.
- Verified sender identity, so a parent can trust a message is genuinely from the school and not an impostor.
- Verified participants in online classes and meetings, so everyone on the call is who they say they are.

PRACTICAL STEPS ANY SCHOOL CAN TAKE

1. Set one official channel
Tell every family which channel the school uses for money and personal data, and that it will never switch to a sudden new email or number.

2. Verify before you pay
Any request for a payment or bank-detail change is confirmed by a call back to a known school number, never a reply to the message.

3. Use verified sender identity
Send school messages on a channel where parents can confirm the sender is really the school, so a fake is easy to spot.

4. Protect online classes
Admit only verified participants to online lessons and meetings, so a stranger cannot slip into a class.

5. Teach the checklist
Share the 12-point checklist with staff, students and parents. One short lesson closes the most common openings.

6. Name a point of contact
Give families one named person to ask "is this really from you?" so checking is quick and normal, not awkward.

Schools interested in the Protected School program can start with the free ProtectMyCalls base and reach the team through protectmycalls.com. The program is designed for the Asia-Pacific region first.

APPENDIX · REPORTING

09 Where to report a scam

Reporting helps you and helps others: it feeds the official data in this report and can support recovery. Use the official channel for your region.

REGION	WHO TO CONTACT	OFFICIAL CHANNEL
United States	FBI IC3 (internet crime) · FTC (consumer fraud)	ic3.gov · reportfraud.ftc.gov
United Kingdom	Action Fraud (England, Wales, NI) · advice via NCSC	actionfraud.police.uk · ncsc.gov.uk
European Union	Your national police or CERT · EU guidance via ENISA / Europol	europol.europa.eu · enisa.europa.eu
Australia	Scamwatch / National Anti-Scam Centre	scamwatch.gov.au
Singapore	ScamShield · Police anti-scam hotline 1799	scamshield.gov.sg
Hong Kong	Police CyberDefender · Anti-Deception hotline 18222	cyberdefender.hk
Japan	National Police Agency cyber / local police	npa.go.jp/cyber
South Korea	KISA / KrCERT · fraud hotline 118	boho.or.kr
Canada	Canadian Anti-Fraud Centre	antifraudcentre.ca

HOW PROTECTMY HELPS

Privacy and verified identity, in one account

ProtectMyCalls

Free, end-to-end encrypted calls and chat, with verified caller identity so you know who is really calling.

ProtectMyMail

Encrypted email with verified senders, so a genuine message stands apart from a fake one.

ProtectMyConference

Encrypted meetings where you can verify every participant before you share anything.

Honest about what this does. Our apps do two things: they keep your communication end-to-end encrypted, and they let you confirm who is really contacting you. They do not scan your messages, analyse voices or detect scams for you. Spotting a scam is still down to you, which is exactly why the checklist on page 8 matters.

Start free with ProtectMyCalls

One account also unlocks ProtectMyMail, ProtectMyConference and more.

METHODOLOGY AND SOURCES

10 How this report was made

Methodology. Every figure in this report is drawn from an official government body, a law-enforcement agency, a national regulator, or a recognised anti-scam organisation, and each is cited with its source and year below. Where a figure was converted to US dollars for the chart on page 4, this is for visual scale only and is marked "approximate"; the native-currency figures and their sources are listed here. We did not estimate, model or combine numbers to create new ones.

Please read this honestly. The figures here reflect reported data only. Many scams are never reported, so the real totals are higher than any number shown. Comparisons between countries are indicative, not exact, because each body defines and counts scams differently. This report is general safety information, not legal or financial advice. No tool and no habit can keep anyone completely safe; privacy, verified identity and good habits together are your best protection, not a guarantee. **Last updated: November 2026.**

FULL SOURCE LIST

1. **FBI Internet Crime Complaint Center (IC3)**, 2025 Internet Crime Report (released April 2026): US$20.877bn reported losses, 1,008,597 complaints, investment fraud US$8.6bn. ic3.gov/AnnualReport
2. **FBI IC3**, annual Internet Crime Reports 2020 to 2024, used for the multi-year trend (US$4.2bn in 2020 to US$16.6bn in 2024). ic3.gov
3. **US Federal Trade Commission (FTC)**, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024" (March 2025): investment US$5.7bn, impostor US$2.95bn, government impostor US$0.79bn, job/business US$0.75bn. ftc.gov
4. **Global Anti-Scam Alliance (GASA) and Feedzai**, Global State of Scams 2025 (October 2025): 46,000 adults across 42 countries, 57% encountered a scam, 23% of those scammed lost money, an estimated US$442bn lost globally, shopping scams most common. gasa.org
5. **Anti-Phishing Working Group (APWG)**, Phishing Activity Trends Reports Q1 to Q4 2025: 3.8 million phishing attacks in 2025; quarterly 1,003,924 / 1,130,393 / 892,494 / 853,244. apwg.org/trendsreports
6. **EU Agency for Cybersecurity (ENISA)**, Threat Landscape 2025 (October 2025, covering July 2024 to June 2025, 4,875 incidents): phishing about 60% of intrusions, vulnerability exploitation 21.3%. enisa.europa.eu
7. **UK Action Fraud**, 2024 fraud data (reported 2025): about £2.3bn reported lost across 318,848 reports; advice via the National Cyber Security Centre. actionfraud.police.uk · ncsc.gov.uk
8. **Singapore Police Force**, Annual Scams and Cybercrime Brief 2024 (February 2025): over S$1.1bn lost, up 70.6%, across 51,501 scam cases. police.gov.sg · scamshield.gov.sg
9. **Japan National Police Agency (NPA)**, 2024 figures: record ¥126.8bn lost to social-media investment and romance scams; phone-based "special fraud" losses of ¥71.9bn. npa.go.jp
10. **Hong Kong Police Force**, 2024 crime figures: HK$5.13bn lost to technology crime across 33,903 cases; deception the main driver of the overall crime rise. police.gov.hk · cyberdefender.hk
11. **South Korea National Police Agency**, 2024 voice-phishing data: about KRW 854.5bn lost, nearly double 2023. boho.or.kr (KISA / KrCERT)
12. **Australia National Anti-Scam Centre (ACCC)**, Targeting Scams 2024 (2025): reported losses down almost 26% to about A$2.03bn; reports down 17.8%. nasc.gov.au · scamwatch.gov.au
13. **Hong Kong Police / SCMP / CNN / Financial Times**, 2024 reporting of the Arup deepfake video-call case (about HK$200m / US$25m). police.gov.hk
14. **FBI public service announcement (December 2024) and FTC consumer alerts**, guidance on AI voice-cloning "family emergency" scams and family safe words. ic3.gov · consumer.ftc.gov

ProtectMyDataSolutions · The 2026 Scam-Safety Report · First edition · Compiled November 2026 from the official sources above.