ProtectMyDataSolutions / Scam-Safety

FREE GUIDE · 2026 EDITION

The 2026 Scam-Safety Report

How to spot a fake email or call, and protect your family. A short, honest guide to the tricks scammers use now, and the simple habits that stop them.

Scams are rising and getting more convincing. Fake emails copy a real brand to the pixel, callers can spoof a trusted number, and a message can push you to act before you have time to think. The good news is that almost every scam depends on the same thing: getting you to trust the wrong sender and move fast. This guide shows you how to spot that, slow it down, and keep your family and your school community safe.

THE NUMBERS

What the official data actually says

GLOBAL

US$16.6 billion

reported lost to online crime in the US in 2024, up about 33% on the year, across 859,532 complaints. Phishing and spoofing was the most reported crime type.

Source: FBI Internet Crime Complaint Center (IC3), 2024 Internet Crime Report (2025).

GLOBAL

About 1 in 4

adults surveyed said they lost money to a scam in the past year, and roughly 7 in 10 had encountered one. Based on about 46,000 adults across 42 countries.

Source: Global Anti-Scam Alliance (GASA) and Feedzai, Global State of Scams 2025 (October 2025).

GLOBAL

3.8 million

phishing attacks observed worldwide across 2025, with a single quarter peaking above 1.1 million. Phishing remains the most common first step in a scam.

Source: Anti-Phishing Working Group (APWG), Phishing Activity Trends Reports, 2025.

ASIA · SINGAPORE

S$1.1 billion

lost to scams in Singapore in 2024, up 70.6%, across 51,501 cases. In 82.4% of cases, victims were manipulated into transferring the money themselves.

Source: Singapore Police Force, Annual Scams and Cybercrime Brief 2024 (February 2025).

ASIA · HONG KONG

44,480 cases

of deception reported in Hong Kong in 2024, up 11.7% on the year. Impersonation of online customer service, banks and officials was a major driver.

Source: Hong Kong Police Force, 2024 crime figures.

ASIA-PACIFIC · AUSTRALIA

Down 25.9%

Reported scam losses fell to about A$2.03 billion in 2024, the first drop in years. Proof that awareness and coordinated action can turn the curve.

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

These figures reflect reported cases only, so the real totals are higher. We cite them to show the scale and the trend, not to alarm you. The point of the next pages is simple: most of this is preventable with a few habits.

HOW MODERN SCAMS WORK

Four patterns behind almost every scam

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. The display name is easy 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 delivery company, the police or a government office. Numbers and caller names can be spoofed, so a familiar number on the screen is not proof of who is really on the line.

3 **Urgency and payment pressure.**
"Act now or your account is closed." "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, or a call where a stranger claims to be a colleague. Treat unexpected invites and links the same way you treat unexpected callers.

THE CHECKLIST

12 habits that stop most scams

Print this, or keep it on your phone. If a message or call fails even one of these, stop and check before you act.

1. Check the real email address, not just the display name.
2. If a message pushes you to act fast, slow down. Urgency is the tell.
3. Call back on a number you already have, never the one in the message.
4. Confirm any money or data request on a second, separate channel.
5. Never share one-time passcodes or login codes with anyone, ever.
6. Treat gift-card, crypto or "safe account" requests as scams.
7. Check where a link really goes before you tap; when unsure, type the address yourself.
8. Verify who is really contacting you. A familiar name or logo is not proof.
9. 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.

FREE FOR SCHOOLS

FOR SCHOOLS

Keep school communication private and verified

Schools are a favourite target because they carry parents' trust and children's data. Through the Protected School program, free for schools, a school can keep its everyday communication both private and verifiable:

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

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 real 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 keep your communication private and 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 above matters.

Start free with ProtectMyCalls

One account also unlocks ProtectMyMail, ProtectMyConference and more.

SOURCES

FBI IC3, 2024 Internet Crime Report (2025). ic3.gov

Global Anti-Scam Alliance (GASA) and Feedzai, Global State of Scams 2025. gasa.org

Anti-Phishing Working Group (APWG), Phishing Activity Trends Reports, 2025. apwg.org

Singapore Police Force, Annual Scams and Cybercrime Brief 2024. police.gov.sg

Hong Kong Police Force, 2024 crime figures. police.gov.hk

Australia National Anti-Scam Centre, Targeting Scams 2024. nasc.gov.au / scamwatch.gov.au

More official help and current scam alerts: US CISA (cisa.gov) and FTC consumer alerts (consumer.ftc.gov); UK Take Five (takefive-stopfraud.org.uk) and Action Fraud; Australia Scamwatch (scamwatch.gov.au); Singapore ScamShield (scamshield.gov.sg); Europol (europol.europa.eu).

ProtectMyDataSolutions · The 2026 Scam-Safety Report. Compiled November 2026 from the official sources listed above. This guide is general safety information, not legal or financial advice. Figures reflect reported data for the years stated and are attributed to their source. No tool can keep anyone "100% safe"; good habits plus privacy and verified identity are your best protection.