



Doxxed, Stalked or Impersonated?

What to do in Singapore

Calm, plain-English steps: what the law
says and where to get help

FREE GUIDE

Philip Choo · AI90S

Contents

<u>Read this first</u>	3
<u>1. The first 24 hours</u>	5
<u>2. Doxxing: when someone posts your personal details</u>	9
<u>3. Online harassment and bullying</u>	13
<u>4. Stalking</u>	16
<u>5. Someone is pretending to be you</u>	19
<u>6. When the account is anonymous</u>	22
<u>7. Scams and getting money back</u>	25
<u>8. Where to get help</u>	29
<u>9. The latest patterns</u>	32
<u>10. What is different in Malaysia</u>	35
<u>Your evidence log and report templates</u>	38
<u>About the author</u>	41

Read this first

If you are reading this because something is happening to you right now, start here.

If you are in danger, or someone has threatened to hurt you, call the police on 999. Everything else in this book can wait.

If you are safe but shaken, that is normal. Having your address posted online, being followed, or finding a fake account using your face is frightening, and it is not your fault. You did not cause it by being online. The people who do these things count on you feeling alone and not knowing what to do. This book is here so that you know what to do.

What this book is

A short, calm guide for ordinary people in Singapore. It explains, in plain English:

- what to do in the first 24 hours;
- what the law says about doxxing, harassment, stalking and impersonation;
- what to do when you do not know who is behind an account;
- what to do if a scam has taken your money;
- where to get help, most of it free.

Every chapter ends with a short box called **What you can do today**. If you only read those boxes, you will still know your next step.

What this book is not

It is general information, not legal advice. The law changes, and your situation is your own. If you are thinking about going to court, speak to a lawyer. Chapter 8 lists free and low-cost places to start.

Where this book states the law, it names the Act and the section, so that you or your lawyer can check it on Singapore Statutes Online (sso.agc.gov.sg). The law is stated as it

stood on the date of this edition.

How to use it

You do not need to read it in order. Find the chapter that matches what is happening:

What is happening	Go to
It just happened and I do not know where to start	Chapter 1
Someone posted my address, phone number or photos	Chapter 2
Someone keeps sending messages, insulting or threatening me	Chapter 3
Someone is following me, watching me, or turning up	Chapter 4
Someone is pretending to be me, or made fake images of me	Chapter 5
I do not know who is doing it	Chapter 6
I lost money to a scam	Chapter 7
I need someone to talk to, or a lawyer	Chapter 8
What is happening more often lately	Chapter 9
The other person is in Malaysia	Chapter 10

At the back you will find a one-page evidence log and three short report templates you can copy.

1. The first 24 hours

When something like this happens, the urge is to do everything at once: reply, report, delete, tell everyone. Slow down. The order you do things in matters more than how fast you do them.

Step 1: Make sure you are safe

If anyone has threatened violence, has turned up where you live or work, or you feel you are in danger, **call 999**. You do not need proof first. Tell a person you trust what is happening, today.

If your home address has been posted, think about who else lives with you and let them know. Simple steps help: keep your door locked, do not open it to people you do not know, and vary your route for a few days if you can.

Step 2: Do not reply

It is natural to want to defend yourself, explain, or hit back. Please do not, at least not yet.

- Replying often makes it worse. It shows the other person they have reached you.
- Anything you write can be screenshotted and used against you.
- **Posting the other person's name, photo or workplace to shame them can itself be an offence.** The law that protects you also applies to you. Chapter 2 explains why.

Step 3: Save it before you report it

This is the step people most often get wrong. When you report a post, the platform may take it down. That is good, but once it is gone, so is your proof.

So before you report anything, save it:

- **Take screenshots** of the post, message or profile. Make sure the screenshot shows the account name, the date and time, and as much of the page as possible.
- **Copy the link** (the web address) of each post and profile. On a phone, use “Share” then “Copy link”.
- **Save the whole conversation**, not only the worst message. The pattern matters.
- **Write down what happened** in your own words, with dates and times. Use the evidence log at the back of this book.
- Keep everything in one folder, and send a copy to yourself by email so it is stored somewhere else too.

Do not edit or crop the screenshots. Keep the originals.

Save it so it counts: records someone else keeps

A screenshot is your own record, and the other side can say you changed it. A record kept by someone with no part in the dispute is harder to argue with. Singapore’s Evidence Act 1893, section 116A(2), lets a court presume that a record kept in the ordinary course of business by a person who is not a party to the case is authentic. Your own screenshot does not get that head start. It is still worth keeping; it just needs company.

You already create some of those records by doing the steps in this chapter in order:

- **Your report to the platform.** The platform keeps its own record of what you reported and when. Screenshot the confirmation or reference number.
- **Your police report** and its report number.
- **Your application to the Online Safety Commission**, if you make one.
- **A witness.** Someone you trust who saw the post can note the date, time and link in their own words.

Do not post the material anywhere yourself to “preserve” it, and do not copy it to public archive websites: a public copy spreads it further, many archives’ terms forbid storing personal data about anyone, and it can outlive the original. If the matter is heading to court, a lawyer can ask the platform to preserve its records.

None of this guarantees that a court will accept anything, and it does not replace reporting. It simply makes your record harder to dispute.

Step 4: Report it, in the right order

Once you have saved everything:

1. **Report the post or account to the platform**, using its own report button. Choose the reason that fits best (harassment, privacy, impersonation).
2. **Make a police report** if you have been threatened, followed, or your personal details have been posted to harass you. You can make a report online through the Singapore Police Force's e-services, or at any neighbourhood police centre. Keep the report number.
3. **Consider the Online Safety Commission**, the government body that can order harmful posts to be taken down. Chapter 2 explains when and how.

Step 5: Protect your accounts

- Change your passwords, starting with your email, and turn on two-step sign-in (the code sent to your phone or app).
- Check who can see your profile, your friends list and your posts. Make them private for now.
- Ask friends and family not to share or comment on the posts, even to defend you. Every share spreads it further.

Step 6: Look after yourself

Being targeted online is stressful, and the stress is real even if no one has touched you. Talk to someone you trust. If it is affecting your sleep, your work or your safety, Chapter 8 lists free support lines, including ones that specialise in online harms.

What you can do today

1. If you are in danger, call 999.
2. Do not reply.
3. Screenshot everything, with the account name, date and link showing.
4. Start the evidence log at the back of this book.
5. Then report to the platform, and to the police if you were threatened or your details were posted.

2. Doxxing: when someone posts your personal details

“Doxxing” means posting someone’s personal details online so that others can find, contact, shame or hurt them. It might be your home address, your phone number, your workplace, your children’s school, or photos of you or your front door.

In Singapore, doxxing to harass or endanger someone is a crime. And since 29 June 2026, there is a government body that can order the post taken down quickly: the Online Safety Commission.

Doxxing is now the harm people report most. In the Commission’s first two months, from 29 June to 31 August 2026, it received more than 500 reports, and doxxing was involved in 44% of the eligible ones. The youngest victim was 7.

What the law says

The Protection from Harassment Act 2014 (often called POHA) covers doxxing in two ways.

Posting your details to harass you (section 3(1)(c)). It is an offence to publish your “identity information”, or that of someone related to you, intending to cause harassment, alarm, distress or humiliation, if it does cause it. The maximum is a \$5,000 fine, 6 months in prison, or both.

Posting your details to put you in danger (section 5(1A)). It is also an offence to publish your identity information intending, or knowing it is likely, to make you fear violence, or to make it easier for others to use violence against you.

“Identity information” is wide. It covers your name, address, phone number, email, NRIC number, photos and videos, and details of your family, job or school. Small pieces that seem harmless on their own count once they are put together to point to you.

The fastest route: the Online Safety Commission

The Online Safety Commission (OSC) can tell the person who posted, the admin of a group, or the platform itself to take the post down, stop sharing it, or restrict the account. Ignoring the Commission's direction is a criminal offence.

For doxxing, you can go straight to the OSC. You do not have to report to the platform first or wait.

- **Report online** at report.osc.gov.sg. There is no fee.
- You will need Singpass or your NRIC or long-term pass.
- **Save your evidence first**, because the post may disappear once action is taken.
- For help with the form, the OSC lists the IMDA contact centre, 6377 3800, during office hours.

Who can report: the victim must be a Singapore citizen, permanent resident or long-term pass holder. A parent or guardian can report for a child under 18. Someone else can report for you with your written permission.

The court routes

The OSC deals with the post. The courts deal with the person.

- **A Protection Order (POHA section 12)** orders the person to stop. If there is urgent risk, you can ask for an **Expedited Protection Order (section 13)**. The court says this hearing is generally within 2 working days of filing.
- Most people file without a lawyer, through the Protection from Harassment Court's simplified process on the Community Justice and Tribunals System (CJTS). The filing fee for a protection order is \$30.
- **Damages:** you can also claim money for the harm (POHA section 11), and since 29 June 2026 there is a separate claim for doxxing under the new Online Safety (Relief and Accountability) Act 2025. You do not need to report to the OSC before going to court.

A court order runs against a named person. If you do not know who is behind the account, see Chapter 6.

The trap: do not doxx them back

It is very tempting to post the other person's name, photo or workplace so that everyone knows who they are. **Do not.** The law applies to everyone. If you post their details to shame or frighten them, you may commit the same offence, and your own case becomes much harder.

The same goes for asking people online to "find out who this is". Let the OSC, the police and the courts do that.

You can dox someone without meaning to

Doxxing is not only something done to you. When you post about a bad experience with another person, such as a break-up, a rude seller or a neighbour, small clues can be enough for strangers to work out who they are: a nickname, a block number, a nearby shop, a screenshot with a name half hidden.

In one case reported by CNA in October 2026, a young woman posted a long video about a break-up. She used nicknames and left out addresses, but viewers still pieced together where another person in the story lived from details such as a nearby restaurant. The Online Safety Commission contacted her and told her the neighbourhood references had to go if the video stayed up. She took it down. Looking back, she agreed the Commission was right to step in.

Before you post about anyone:

- **Ask what a stranger could work out** from your post, not only what you have written outright.
- **Leave out places, workplaces, schools and photos** that point to the other person.

- **Do not share or comment** on other people's posts that expose someone. Every share spreads the harm further, even if you did not write the post.

What you can do today

1. Screenshot the post with the account name, date and link showing.
2. Report it to the OSC at report.osc.gov.sg. For doxxing you do not need to wait for the platform.
3. Report to the platform as well.
4. Make a police report if the post puts you in danger or invites people to find you.
5. Do not post the other person's details, however angry you are.

3. Online harassment and bullying

Harassment is being targeted again and again: insults, threats, sexual comments, a group chat set up to mock you, messages that will not stop. It can happen to anyone, at any age. It is not “just online”, and you do not have to put up with it.

What the law says

The Protection from Harassment Act 2014 (POHA) makes two kinds of harassment an offence.

- **Intentional harassment (section 3).** Using threatening, abusive, insulting, sexual or indecent words, behaviour or messages, intending to cause harassment, alarm, distress or humiliation, and causing it. Up to a \$5,000 fine, 6 months in prison, or both.
- **Harassment without proving intent (section 4).** The same kind of words or messages, seen or heard by someone likely to be caused harassment, alarm, distress or humiliation. Up to a \$5,000 fine.

“Humiliation” was added to the law on 29 June 2026. Being humiliated online, for example by having embarrassing images or posts spread about you, now counts.

If someone is spreading lies about you, POHA also lets a court order the person to stop publishing a false statement, or to publish a correction, and can order a platform to disable access to it (sections 15A to 15D).

Step 1: Report to the platform first

For harassment, **report to the platform before you go to the Online Safety Commission.** Use the platform’s own report button, and screenshot your report or the platform’s reply. You will need it.

Step 2: If the platform does not act within 24 hours, go to the OSC

If the platform does not respond, or its response does not solve the problem, **within 24 hours**, you can report to the Online Safety Commission (OSC) at report.osc.gov.sg. There is no fee. The OSC can direct the person, the group admin or the platform to remove the material, stop the conduct or restrict the account.

The OSC asks for proof that you reported to the platform first, so keep that screenshot.

Step 3: The court, if it continues

If the harassment continues or you know who is doing it, you can apply to the Protection from Harassment Court for a **Protection Order**, and an **Expedited Protection Order** if it is urgent. The court says expedited hearings are generally held within 2 working days. Most people apply themselves through the simplified process on CJTS; the filing fee is \$30. You can also claim damages.

If you are a parent

Children and teenagers are often targeted by people they know: classmates, former friends, group chats. About 17% of the eligible reports to the OSC in its first two months involved a victim under 18.

- **Stay calm and listen.** Many young people do not tell adults because they fear their phone will be taken away. Make it clear that telling you will not get them into trouble.
- **Save the evidence together** before anything is deleted.
- **Report to the platform**, and tell the school if classmates are involved.
- **You can report to the OSC for your child** if they are under 18.
- For children 13 and under, **Tinkle Friend** (1800 2744 788) offers a listening ear. Chapter 8 lists more support.

What not to do

- Do not reply in anger, and do not post about the person to get back at them.

- Do not create fake accounts to watch them or confront them.
- Do not delete the messages, even if they upset you. Save them in a folder you do not have to look at.

What you can do today

1. Screenshot the messages, with names, dates and links.
2. Report to the platform and screenshot your report.
3. If nothing happens within 24 hours, report to the OSC at report.osc.gov.sg.
4. If you know who it is and it continues, consider a Protection Order through the Protection from Harassment Court.
5. Tell someone you trust.

4. Stalking

Stalking is when someone keeps turning up in your life when you do not want them to. It can be online, offline, or both: following you, waiting outside your home or office, watching your social media and messaging you about where you have been, tracking your location, or contacting your friends and family about you.

If you think someone is following you right now, go to a busy public place and call 999. If it is not safe to talk, you can SMS 70999.

What the law says

Unlawful stalking is an offence under section 7 of the Protection from Harassment Act 2014 (POHA). It needs three things:

1. a **course of conduct** made up of acts associated with stalking;
2. that conduct **causes you harassment, alarm, distress or humiliation**; and
3. the person **intended this, or knew or ought to have known** it was likely.

The law gives examples of acts associated with stalking, including following you, contacting you or others about you, loitering near your home or workplace, and keeping you under surveillance.

The maximum is a \$5,000 fine, 12 months in prison, or both (section 7(6)).

A “course of conduct” can be shorter than you think. It can be a single long occasion (section 7(10)). In one reported case, following a woman for about three hours on a single afternoon was enough.

Online stalking and the Online Safety Commission

Online stalking, such as repeatedly tracking and messaging you about your movements, is one of the harms the Online Safety Commission (OSC) handles. As with harassment,

report to the platform first. If it does not act adequately within 24 hours, report to the OSC at report.osc.gov.sg.

Getting a court order

A **Protection Order** under POHA section 12 can order the person to stop: not to approach you, contact you, or post about you. If you are at urgent risk, apply for an **Expedited Protection Order** under section 13. The court says these hearings are generally within 2 working days of filing. You can apply yourself through the Protection from Harassment Court's simplified process on CJTS (filing fee \$30).

An order only takes effect once it is served on the other person. Breaking an order is itself an offence, so call the police if it happens.

Keeping yourself safe

- **Tell people.** Let family, friends, your workplace security and your building management know, and share a photo of the person if you have one.
- **Check your phone.** Review which apps can see your location, and who you share your location with. Check your accounts for devices you do not recognise and sign them out.
- **Check your belongings** if you think you are being tracked. Tracking devices can be small. If you find one, do not destroy it: take it to the police.
- **Vary your routine** for a while, and do not post your location or plans in real time.
- **Write everything down** in your evidence log: dates, times, places, what the person did, and who else saw it.

What not to do

- Do not confront the person alone.
- Do not follow or watch them back, or ask friends to. Even with good reasons, it can look like the same conduct.
- Do not install tracking or spying apps on anyone else's phone. That can be a serious offence.

What you can do today

1. If you feel in danger, call 999 (or SMS 70999 if you cannot talk).
2. Start your evidence log, with every date, time and place.
3. Tell people around you, and check your phone's location sharing.
4. Make a police report.
5. Ask the court for a Protection Order, or an Expedited one if the risk is urgent.

5. Someone is pretending to be you

It is a horrible feeling: a profile with your name and photos, messaging your friends, asking them for money, or posting things you would never say. Or worse, a fake intimate image of you, made with editing or AI tools, being shared.

This chapter covers three situations: fake accounts, fake or real intimate images, and threats to share images unless you pay (often called “sextortion”).

A fake account in your name

Step 1: Save it. Screenshot the profile, its posts and any messages it has sent, with the link and the account name showing. Ask friends who were contacted to screenshot what they received.

Step 2: Warn people. Post on your real account, or message your contacts, that a fake account exists and they should not accept requests, reply or send money. Do not link to the fake account itself.

Step 3: Report it to the platform. Every major platform has an “impersonation” or “pretending to be me” report option. Some ask for a photo of your ID; send it only through the platform’s own official form.

Step 4: Report to the police if the account is being used to ask people for money, to cheat anyone, or to harass you.

What about the Online Safety Commission? The new law defines “online impersonation” as a harm, but **as of this edition, it is not yet one of the harms the Commission handles.** It is in a group of harms the government says will be brought in progressively. Until then, use the platform, the police, and the protection orders in Chapter 3 if the impersonation is harassing you. Check osc.gov.sg for updates.

Intimate images: real or fake

If someone shares, or threatens to share, an intimate image or video of you:

- **This is a serious crime.** Under section 377BE of the Penal Code, distributing, or threatening to distribute, an intimate image or recording without consent can mean up to 5 years in prison, a fine, caning, or a combination.
- **Fake images count.** Since 17 August 2026, an “intimate image” includes one that has been altered or generated, for example by AI, to look like you.
- **A threat is enough.** The police do not need to prove the image exists.

Go straight to the Online Safety Commission. Intimate image abuse is one of the five harms it handles now, and you do not need to report to the platform first. Report at report.osc.gov.sg. If you were under 16 in the image, or it looks like it shows someone under 16, report it as image-based child abuse.

Make a police report as well.

On saving evidence: save the link, the account name, the date and the message that came with it. You do not need to keep collecting copies of the image itself; tell the police and the OSC where it is.

Sextortion: “pay or I will share it”

Someone, often a stranger you met online, says they have an intimate image or video of you and will send it to your family, friends or employer unless you pay.

1. **Do not pay.** Paying almost never ends it. It tells them you will pay again.
2. **Stop replying,** but do not delete the conversation.
3. **Save everything:** their account name, the messages, any payment details they gave you.
4. **Report to the police.** Extortion is a serious offence (Penal Code section 384), and so is threatening to share an intimate image (section 377BE).
5. **Report to the OSC** at report.osc.gov.sg, and to the platform.

6. Talk to someone. This is designed to make you feel ashamed and alone. You are the victim of a crime, not the one who did something wrong. Chapter 8 lists people you can call, any time.

What you can do today

1. Screenshot the fake account or messages, with links and dates.
2. Warn your contacts not to reply or send money.
3. Report the account to the platform as impersonation.
4. If intimate images are involved, report to the OSC at report.osc.gov.sg and to the police. Do not pay anyone.
5. Talk to someone you trust, or call one of the lines in Chapter 8.

6. When the account is anonymous

Often the account harassing you has no real name, no photo and was created a few days ago. You may feel stuck: how do you stop someone when you do not know who they are?

Here is the good news. **Getting the post removed does not need a name.** Getting a court order against the person does. Deal with the post first.

Step 1: Get the post removed

You do not need to know who posted something to have it taken down.

- **Report to the platform.**
- **Report to the Online Safety Commission** at report.osc.gov.sg. For doxxing and intimate images you can go straight there; for harassment and stalking, wait 24 hours after your platform report (Chapters 2 and 3). The OSC can direct the platform to disable access or restrict the account, whoever is behind it.
- **Report to the police.** The police can investigate without you naming anyone.

Step 2: Asking the Online Safety Commission for the person's identity

Since 29 June 2026, there is a new route. Under section 53 of the Online Safety (Relief and Accountability) Act 2025, the Commissioner of Online Safety may give a victim the identity information or contact details of the person reasonably suspected of causing the harm.

It is not automatic. You must:

- **apply in writing**, for a purpose allowed by the rules (for example, to take legal action);
- satisfy the Commissioner that the person is reasonably suspected of the harm;
- pay a fee; and

- **apply within 12 months** of the harm, or of when you became aware of it.

The Commissioner can attach conditions to how you use the information. **Breaking those conditions is an offence**, with a fine of up to \$20,000, up to 12 months in prison, or both. The information is for your case, not for posting online.

Step 3: Asking a court

The older route is to ask the court, through a lawyer, to order a platform or telco to hand over what it holds about an account before you sue (the Rules of Court 2021 allow this). Courts weigh this carefully, including the privacy of other users, and they cut down requests that are too broad. A narrow request backed by a clear, dated record of what happened has the best chance.

Why your evidence log matters so much here

Every one of these routes asks you to show what happened, when, and from which account. A tidy evidence log with screenshots and links is what turns “someone is bothering me” into a request an official or a judge can act on. Start it on day one.

Do not try to unmask them yourself

When you are frightened and angry, it is tempting to hunt for the person yourself, ask a friend who is “good with computers”, or post the account and ask the internet who it is. Please do not.

- **Posting the account and asking people to identify the owner** can be doxxing in itself, especially if someone guesses the wrong person.
- **Repeatedly contacting them** to demand they stop can look like the harassment you are complaining about.
- **Hacking into an account or device** to find out who is behind it is a crime under the Computer Misuse Act, whatever the reason.

If you want professional help, look for a licensed investigator who works only by lawful means (Chapter 8 explains how to check). A lawful investigator will help you preserve evidence and find what can properly be found, and will refuse to hack or buy leaked data.

What you can do today

1. Report the post to the platform and the OSC. A name is not needed.
2. Make a police report.
3. Keep building your evidence log.
4. If you need the person's identity for legal action, note the 12-month deadline to apply to the Commissioner.
5. Do not post the account and ask others to identify it.

7. Scams and getting money back

If you have just realised you sent money to a scammer, or someone has used your banking login, **call your bank's 24-hour hotline now** and ask them to block your account and any further transfers. Then make a police report. Speed matters more than anything else in this chapter, because scammers move money within minutes.

Once you have done that, this chapter explains, honestly, what usually happens next. Some of it is hard to hear. It is better to know now than to wait months for a refund that was never coming.

Three words that sound alike but are not

Frozen is not recovered. When the police freeze a bank account that received scam money, the money is stopped where it is. That is good, because it cannot move further. But a freeze does not decide who gets the money. That is decided later, by a court, under section 370 of the Criminal Procedure Code 2010, and it goes to “the person entitled to possession”, which is a legal question. If one account received money from many victims and holds less than they all lost, they may have to share what is left.

Forfeited is not recovered. In some large cases, money and property are forfeited to the State. When that happens, the value goes to the government, not back to individual victims.

Restricted is not recovered either. Under the Protection from Scams Act 2025, in force since 1 July 2025, the police can issue a restriction order that temporarily stops a person's own bank transfers when they believe that person is about to send money to a scammer. It is there to stop you losing money while you are still being deceived. It does not bring back money already sent.

None of this means you will get nothing. It means the realistic hope rests on how fast the money was stopped, and whether it was still in Singapore when it was.

The one route where the bank may have to pay you back

There is one kind of scam where you may be repaid without going to court. It is called the **Shared Responsibility Framework**, set by the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA), in force since 16 December 2024.

Does it cover your case?

It covers phishing in a strict sense. All four of these must be true:

1. the scammer **pretended to be a real business or government body**, such as your bank or a government agency;
2. they contacted you through a **messaging channel**, such as SMS, email, WhatsApp or social media;
3. you **entered your login details on a fake website or app**; and
4. those details were then used for **transactions you did not intend**.

If you were persuaded to send the money yourself, for example to a fake investment, a fake job or someone you met online, **this framework does not cover it**. Credit, debit and charge cards issued in Singapore are also outside it; they have their own rules.

What decides whether you are repaid

The test is not whether you were careless. It is whether your bank, and then your mobile operator, did a set of specific things they are required to do. These include a cooling-off period of at least 12 hours after a new device is set up for your account, real-time alerts, a reporting channel open at all times with a way to block your own account (“kill switch”), and fraud monitoring. For SMS scams, the telco must block fake sender names and filter known scam links.

If the bank missed one of its duties, it is expected to bear the loss in full. If the bank did everything right but the telco missed one of its duties, the telco pays. If neither missed anything, the loss stays with the account holder.

The deadlines

- **Report to your bank as soon as you can, and within 30 calendar days.**
- **Within 3 calendar days of reporting**, give the bank an email address and your supporting evidence, such as the police report and the scam messages.
- **Keep the scam message.** For an SMS scam, keep a screenshot showing the sender, date and time.

The bank is your single point of contact, even if the telco is involved. If you disagree with the bank's decision, you can take it to the Financial Industry Disputes Resolution Centre (FIDReC). Disagreements with a telco's assessment go to IMDA in writing.

Going to court

You may also have a civil claim to get money back from the person who received it. That needs a lawyer, and it is only worth it if the money can still be reached. Before spending anything, ask: where is the money now, and when was that established? If it has already left Singapore, the costs rise sharply and the chances fall.

Be careful of “recovery” offers

After a scam, many victims are contacted by people who promise to get their money back for a fee. **This is very often a second scam**, run by the same people or by others who buy lists of victims. No lawful service can guarantee to recover your money. Never pay an upfront fee to anyone who contacts you out of the blue, and check that anyone offering investigation help is licensed (Chapter 8 explains how).

What you can do today

1. Call your bank's 24-hour hotline and block your account.
2. Make a police report and keep the report number.
3. Screenshot the scam message showing the sender, date and time.
4. If it was phishing, write to your bank within 30 days and send your evidence within 3 days of reporting. Use the template at the back of this book.

5. Ignore anyone who contacts you offering to recover your money for a fee.

8. Where to get help

You do not have to deal with this alone. Most of the help below is free.

Emergencies

Who	How
Police, emergency	999
Police, if it is not safe to talk	SMS 70999
Police hotline, non-emergency information	1800 255 0000

Reporting

What	Where
Online Safety Commission: doxxing, online harassment, online stalking, intimate image abuse, image-based child abuse	report.osc.gov.sg (free). Help with the form: IMDA contact centre 6377 3800, office hours
Police report	Singapore Police Force e-services, or any neighbourhood police centre
Not sure if something is a scam	ScamShield helpline 1799 (24 hours), scamshield.gov.sg
Scam involving your bank account	Your bank's 24-hour hotline, first

Support for victims of online harm

SHECARES, run by SG Her Empowerment (SHE), describes itself as Singapore's first dedicated support centre for victims of online harm. It is for everyone, not only women.

- Call 800 101 4616, or WhatsApp (text only) 8985 5528, Monday to Friday, 9am to 9pm, except public holidays.
- It can help you flag harmful content to platforms, make a report to the Online Safety Commission, and get counselling.
- It runs free legal clinics on the 1st, 3rd and 5th Wednesday of the month, 7pm to 9pm, by appointment.

Someone to talk to

Who	How	When
National Mindline	Call 1771, or WhatsApp 6669 1771	24 hours
Samaritans of Singapore	Call 1767, or WhatsApp (text) 9151 1767	24 hours
Tinkle Friend (children 13 and under)	1800 2744 788	Weekday afternoons
TOUCH Community Services	1800 377 2252	Weekdays, 9am to 6pm

If you are having thoughts of harming yourself, please call 1767 or 1771 now. You matter more than anything anyone has posted.

Going to court without a lawyer

The **Protection from Harassment Court** has a simplified process for people without lawyers, filed online through the Community Justice and Tribunals System (CJTS). Filing a protection order application costs \$30. The court's website, judiciary.gov.sg, has step-by-step guides and a pre-filing assessment tool.

For legal advice, SHECARES's free legal clinics are a good start. Community legal clinics and the Law Society's pro bono services can also help people who cannot afford a lawyer.

If you want an investigator: check the licence first

Sometimes people want professional help to preserve evidence properly or to find out what can lawfully be found. In Singapore, anyone who does investigation work for payment must hold a licence under the Private Security Industry Act 2007.

- **Ask for the licence number**, and check it with the Police Regulatory Department (PRD) before you pay anything.
- An unlicensed investigator commits an offence, and an unlicensed agency cannot recover its fees in court.

What no lawful investigator will do:

- hack into accounts, phones or emails;
- buy or search leaked or stolen databases;
- install tracking or spying apps;
- promise to “unmask” an anonymous account by any means;
- guarantee to recover scam money for an upfront fee.

If someone offers any of these, walk away. You could end up as a suspect yourself, and your evidence may become useless in court.

What you can do today

1. Save the numbers you need in your phone: 999, 70999, 1799, 1767, 1771.
2. If this is affecting you, call SHECARES, Mindline or Samaritans. Talking helps.
3. If you need a lawyer, book a SHECARES legal clinic or a community legal clinic.
4. If you hire an investigator, check the licence before paying.

9. The latest patterns

This chapter is short and dated. It changes with every edition. It uses only official public figures, and never discusses any individual case.

As at October 2026.

Doxxing is the most reported harm

The Online Safety Commission began work on 29 June 2026. In its first two months, to 31 August 2026, it received more than 500 reports and resolved more than 90% of the eligible ones. By type of harm, the eligible reports involved:

Harm	Share of eligible reports
Doxxing	44%
Online harassment	38%
Intimate image abuse	8%
Online stalking	7%
Image-based child abuse	3%

(One report can involve more than one harm.)

What this tells you: doxxing is common, and you are far from alone if it has happened to you. Men and women were affected at nearly equal rates, and victims ranged in age from 7 to 68.

Young people are targets

About 17% of eligible reports involved a victim under 18. The youngest was 7, in a doxxing case. If you are a parent, talk to your children about what to do if their details or photos

are shared, before it happens.

AI-generated fakes

Editing apps and AI tools make it easy to create realistic fake images and videos of real people. The law has started to catch up: since 17 August 2026, fake intimate images made to look like a real person are covered by the same offence as real ones (Penal Code section 377BE). The new online safety law also defines “inauthentic material abuse” (deepfakes that cause distress), but as of this edition the Online Safety Commission does not yet handle it. Chapter 5 explains what to do now.

Doxxing by joining the dots

Doxxing used to mean someone posting your address. Increasingly it happens in pieces. Researchers quoted in a CNA Big Read on 9 October 2026 call this “linkability”: a photo, a workplace, an old username or a location, each harmless alone, which other people combine across platforms until they point to one person. Once the pieces have spread, deleting the original post may already be too late.

The same report describes three patterns worth knowing:

- **The accidental mob.** Someone posts about a personal grievance without naming anyone, and viewers do the identifying for them.
- **The wrong person.** Online crowds sometimes “identify” the wrong person from a viral video, and an innocent person’s name, photo and employer are spread. A clarification rarely travels as far as the accusation.
- **Faster takedowns.** CNA reports that platforms must now respond to Online Safety Commission notices within 48 hours, or 6 hours for the most serious image abuse, compared with five days or more before the Commission existed.

What this tells you: before sharing a post that “exposes” someone, stop. You may not know the full story, it may be the wrong person, and every share adds to the harm.

What is coming

The government has said eight more categories of online harm will be brought under the Online Safety Commission progressively. They include online impersonation, deepfakes (“inauthentic material abuse”), incitement of violence, and sharing private information without consent. No dates have been announced. When they arrive, the next edition of this book will explain them; sign up at ai9os.com to hear when it does.

What you can do today

1. Check your own privacy settings: who can see your photos, school, workplace and location.
2. Talk to your children about what to do if their details or photos are shared.
3. Be careful which apps you upload clear photos of your face to.

10. What is different in Malaysia

Many people in Singapore have family, friends, work or a former partner across the Causeway. If the person harassing you is in Malaysia, or you live there, here is what is different. It is short on purpose: Malaysian law is its own system, and anything beyond these basics needs a Malaysian lawyer.

Doxxing and bullying are offences in Malaysia too

In 2025 Malaysia added new bullying and harassment offences to its Penal Code, in sections 507B to 507G (Penal Code (Amendment) Act 2025, Act A1750). They are reported to have taken effect on 11 July 2025.

Two of them deal with doxxing, which the Act describes as publishing, circulating or making available someone's "identity information":

- **Section 507E:** doing this to cause a person harassment, distress, fear or alarm. Up to 3 years in prison, a fine, or both.
- **Section 507F:** doing this to make a person believe harm will be caused to them, or to make it easier for others to harm them. Up to 1 year, a fine, or both.

"Identity information" means any information that identifies, or claims to identify, a person (section 507G). The Act's own example is posting a former partner's intimate photos without consent.

The other sections cover threatening, abusive or insulting words and messages more generally (sections 507B to 507D), including provoking someone to harm themselves.

Stalking

Malaysia's Penal Code also has a stalking offence, section 507A, added in 2023. It is reported to carry up to 3 years in prison, a fine, or both, and the court can reportedly issue

a protection order against a person investigated or charged with stalking. Ask a Malaysian lawyer or the police how that works today before relying on it.

Reporting harmful content

Malaysia's Online Safety Act 2025 places duties on large platforms and messaging services, not on individuals. It does not give you a claim against the person harassing you, but it does give you two places to report:

1. **The platform itself**, through its own report button.
2. **The Malaysian Communications and Multimedia Commission (MCMC)**, through its complaint portal at aduan.mcmc.gov.my.

Scams

If you lost money to a scam involving a Malaysian bank account, call Malaysia's **National Scam Response Centre on 997**. It runs 24 hours a day and asks you to report within 24 hours of discovering the scam. Make a police report as well; treat them as two separate steps.

The cross-border problem

Singapore's police, courts and Online Safety Commission work in Singapore. When the person harassing you is in Malaysia, getting an order made in one country obeyed in the other is slow and uncertain. In practice:

- report to the platform, because platform rules apply wherever the poster is;
- report in the country where you are, and keep the report number;
- if the person is in Malaysia, a report to the Malaysian police and MCMC may also be needed;
- keep one evidence log for everything, so the same record serves both countries.

What you can do today

1. Save the evidence, exactly as in Chapter 1.
2. Report to the platform.
3. Report where you are; if the person is in Malaysia, consider a report there too (MCMC at aduan.mcmc.gov.my, or a Malaysian police station).
4. For a scam involving a Malaysian account, call 997 and make a police report.
5. Speak to a Malaysian lawyer before taking any step in court there.

Your evidence log and report templates

Your evidence log

Copy this table into a notebook, a spreadsheet or your phone's notes. Add one row every time something happens, even if it seems small. A clear, dated record is the single most useful thing you can bring to the police, a platform, the Online Safety Commission or a lawyer.

No.	Date and time	Where (app, website, place)	What happened, in your own words	Link or account name	Screenshot saved?	Someone else's record (platform reference, police report no., witness)	Reported to (and reference number)
1							
2							
3							
4							
5							

Tips

- Write it down the same day, while you remember it clearly.
- Describe what happened, not what you think it means. “He posted my block and unit number at 9.14pm” is stronger than “he is trying to scare me”.

- Keep screenshots in one folder, named with the date, for example 2026-10-09_2114_post.png.
- Note any witnesses, and anyone who told you about a post you did not see yourself.

Template 1: Report to a platform

Most platforms give you a short box to explain. Keep it factual.

I am reporting this account/post for [harassment / sharing my personal information / impersonating me].

Link: [paste the link] Account name: [name] Date I first saw it: [date]

This post shares my [home address / phone number / photos] without my consent. It has led to [strangers contacting me / threats]. I am the person shown. I have kept copies and reported it to the police (report number [number], if you have one).

Please remove it and stop this account from posting about me.

Template 2: Notes for a police report

Bring these notes with you, or use them to fill in the online form.

What happened: On [date], an account called [name] posted my [address / photos / phone number] on [platform]. Since then, [what followed: messages, calls, people turning up].

Who: [The person's name if you know it. If not: "I do not know who runs the account."]

Why I am afraid: [For example: the post invited people to visit my home; I received a threat on (date).]

What I have: screenshots with dates and links; my evidence log; [names of witnesses].

What I have already done: reported to [platform] on [date]; [any other reports].

Template 3: Report to your bank after a scam

Call your bank's 24-hour hotline first, then follow up in writing. See Chapter 7 for the deadlines.

I am reporting unauthorised transactions on my account [last four digits only].

When: [date and time I noticed] **Transactions:** [date, amount, recipient, for each one] **How it happened:** I received a [SMS / WhatsApp / email] on [date] that appeared to be from [bank / agency]. It led me to a website where I entered my [login details / one-time password]. **What I have:** the message (screenshot showing sender, date and time), the link, my police report number [number].

Please block further transactions, investigate under the Shared Responsibility Framework, and confirm in writing. My email address for your reply is [email].

Never send your full card number, password or one-time password in any message, to anyone, including your bank.

About the author

Philip Choo is a licensed private investigator in Singapore and the founder of AI9OS. AI9OS publishes free, plain-English guides on the law that applies to online harms and investigations in Singapore and Asia, at ai9os.com.

AI9OS publishes information; it does not investigate. If you need licensed help with your own situation, such as preserving evidence properly or establishing what can lawfully be found out, that work is done by Spyrrus Tech Pte Ltd, a licensed private investigation agency in Singapore. You can reach Philip there through ai9os.com/contact (choose “Licensed help with a matter”).

Keep this guide current

The law on online harms in Singapore changed a great deal in 2026 and will keep changing. To get a short email when something important changes, sign up at ai9os.com and choose “Personal”.

Share it

This book is free. You are welcome to share it with anyone who needs it, in full and unaltered.

© Philip Choo / AI9OS.COM (UEN 53527859D). Free to share in full and unaltered. Edition of 12 October 2026.