CFM Public Advisory

A public-facing consumer advisory article aimed at raising awareness about eSIM fraud, written in clear, practical language suitable for CFM platforms (website, social media, newsletter, etc.). Tone: direct, preventive, empowering.

Beware of eSIM Fraud: Don't Share Your Login — Not Even with Loved Ones

As technology advances, so do the tactics of fraudsters. One of the fastest-growing threats in Malaysia right now is eSIM fraud where scammers hijack your mobile number by taking advantage of weaknesses in account security and digital self-service platforms. And yes, this can happen even if you never lost your phone.

What is eSIM Fraud?

An eSIM (embedded SIM) is a digital SIM built into your phone that can be activated remotely — no physical card required. While convenient, it also creates an opportunity for fraudsters to take over your mobile number if your telco app login falls into the wrong hands.

Once they hijack your number, they can:

✅ Intercept your SMS OTPs
✅ Access your WhatsApp or social media
✅ Enter your banking apps
✅ Drain your bank account

How It Happens

These cases are becoming more common in Malaysia:

1. Scammer gets your telco app login — often via phishing, leaked passwords, or careless sharing.
2. They log into your telco app, change the registered email to their own.
3. Your telco doesn't alert you or request a verification.
4. Scammer requests an eSIM activation, installs your number on *their* device.
5. You lose network — they gain full control.

All this can happen in under 10 minutes — quietly.

Don't Let This Be You: NEVER Share Your Login

Even with people you trust do not share:

- Your telco app password or login ID
- OTPs sent via SMS or email
- Your IC or bank card photos
- Screenshots of QR codes (especially eSIM setup)

If your account gets compromised, you may be held responsible if your telco believes access was "granted" willingly.

"But I only shared with my partner/family/friend!"
That's still a security risk. Fraud can happen unintentionally, or your shared info might be leaked or misused by someone else.

🧠 **Smart Consumer Tips**

✅ **DO THIS**	🚫 **NEVER DO THIS**
Set strong passwords for telco apps	Reuse the same password across apps
Enable biometric login (Face/Touch ID)	Store password in phone gallery or notes
Read telco email/SMS alerts carefully	Ignore notices about account/email changes
Buy eSIMs from official sources only	Get "cheap roaming eSIMs" from WhatsApp
Contact telco **immediately** if no service	Wait and assume it's a "network issue"

If You're Affected

1. Contact your telco immediately to freeze the number and investigate.
2. Lodge a police report — this is a criminal offense.
3. Report the case to CFM https://www.mcmc.gov.my/ms/make-a-complaint/mcmc-complaint-portal
4. Notify your bank to dispute unauthorized transactions.

What CFM Is Doing

CFM is actively monitoring this growing trend and has raised the issue with service providers. We are urging:

- Mandatory two-factor verification before approving any email or eSIM changes.
- Real-time alerts for sensitive account activities.
- Better consumer education via telco apps and websites.

Final Reminder: Protect Your Digital Identity

Treat your telco login like your bank login.
It gives access to more than just your calls it can unlock your entire financial identity.

Be alert. Stay in control. Never share your telco login not even with loved ones.