Passkeys: Build a Recovery Plan Before Switching

Description

Passkeys reduce phishing risk because there is no password or one-time code to type into a fake page. Before switching an important account, identify where the passkey is stored, how it synchronises, what happens after device loss and which independent recovery route remains.

This guide is for a singapore consumer replacing passwords with passkeys across important accounts. Its job is specific: gain phishing resistance without making one phone or cloud account a single point of failure. Use the table first, then the worked example and checklist; keep any calculation as a labelled estimate until the controlling body or live service confirms it.

passkey recovery plan Singapore: the decision table

Situation	Practical next step
Passkey syncs through a protected platform account	Secure that platform and document its recovery route
Account supports more than one passkey	Register a second trusted device or hardware key
Only recovery is SMS to one phone	Add a stronger independent method if the service allows
Old device will be sold or wiped	Test new-device sign-in before removing the old passkey

The table separates the common branches that lead to different outcomes. It is not a substitute for reading the current source: re-open the cited authority on the day the decision is made, especially where a deadline, rate, eligibility rule, opening condition or safety instruction is involved.

Start with the controlling rule

Passkeys use public-key cryptography and bind sign-in to the legitimate service, making credential interception through a lookalike page much harder than password or OTP entry. CSA MFA-bypass

advisory.

The private credential may live on one device, a hardware security key or a platform sync service. The recovery plan depends on which model the account and device actually use. CSA authentication-method guide.

These two checks define the readerâ??s starting position. Record the date and the facts used, because a later application, booking or dispute is easier to resolve when the original basis is visible.

Apply the rule to the real decision

Secure the Apple, Google, Microsoft or password-manager account that synchronises passkeys. A weak recovery email can undermine a strong sign-in method. CSA MFA-bypass advisory.

Where supported, register more than one passkey: for example, a primary phone and a separate hardware key stored safely. Do not keep every factor in the same bag. CSA authentication-method guide.

Do not compress separate conditions into a single yes-or-no answer. Work through the eligibility, timing, amount and evidence questions in that order, and stop if a live record does not match the assumption.

Build the evidence trail

Keep recovery codes offline and update trusted phone numbers and email addresses. Test that the serviceâ??s account-recovery page is reachable without an already signed-in device. CSA MFA-bypass advisory.

Passkeys do not prevent malware, malicious account recovery or approving an attackerâ??s request. Keep device updates, screen lock and login alerts enabled. CSA authentication-method guide.

Save the relevant confirmation, receipt, official result or case reference. This is not administrative decoration: it is the record that allows the authority, provider or household to reconstruct what happened.

Know the limit of the answer

Remove passkeys from lost, sold or shared devices through the accountâ??s security dashboard. Wiping a phone is important, but the service-side credential list should also be reviewed. CSA MFA-bypass advisory.

Migrate one important account at a time. Test normal sign-in, a second device and the documented recovery route before removing the password or legacy factor where removal is optional. CSA authentication-method guide.

This guide resolves the general task for a Singapore reader. It does not replace an individual notice, contract, clinical assessment, legal advice or an officerâ??s direction at the point of service.

Worked Singapore example

A user stores a bank-adjacent service passkey on a phone synced to a platform account. Before wiping the old phone, the user signs in from the new device, adds a hardware key, prints recovery codes and confirms the recovery email. The old device passkey is then removed from the service dashboard.

The example shows the method, not a promised outcome. Replace its dates, balances, prices, route conditions or personal facts with the readerâ??s own information. Where the example performs arithmetic, it is an editorial calculation and should be reconciled against the live statement, bill or official calculator.

Action checklist

1. Identify where each passkey is stored
2. Secure the sync or platform account
3. Register a second independent passkey where possible
4. Save recovery codes offline
5. Test sign-in on the replacement device
6. Review login alerts and recovery contacts
7. Remove credentials from old or lost devices

Work through the list in sequence. If one item cannot be verified, record the gap and use the official contact route rather than guessing. Keep screenshots only as supporting evidence; the live authority page and issued document remain controlling.

Two original tools in this guide

A passkey storage-and-recovery dependency map. This converts the source material into a reusable decision aid. Copy it into a note or spreadsheet and enter only verified personal inputs.

A before-wipe migration test for old and new devices. This is the final control before an irreversible payment, submission, booking, journey or household decision. It is an editorial framework derived from the sources, not an official form.

Primary-source ledger

Official or primary source	Material claims checked
CSA MFA-bypass advisory	Phishing-resistant authentication, FIDO2 security keys and passkeys.
CSA authentication-method guide	Trade-offs among authentication methods and suitability considerations.

Each inline link sits beside the claim it is intended to support. Both source pages were opened during the evidence pass. If a page is revised after publication, use the latest controlling text and treat this articleâ??s worked examples as historical calculations rather than fresh official advice.

Errors that change the outcome

- Assuming passkeys make account recovery irrelevant
- Keeping every device and key together
- Using an unprotected recovery email
- Wiping the old phone before testing the new one
- Approving an unexpected recovery prompt

The recurring failure is to act on a familiar label without checking its definition. Preserve the original notice, policy wording, booking terms, eligibility record or authority response so that a later review starts from evidence rather than memory.

Continue with the next useful step

For the adjacent task, read recovering Singpass after a phone change. If the decision moves into another stage, continue with checking a suspicious sign-in message. These links were selected for reader progression, not as mechanical category links.

Questions readers ask

Why are passkeys phishing-resistant?

They use cryptographic authentication bound to the legitimate service instead of a secret typed into a page. CSA MFA-bypass advisory.

Should I keep a password?

Follow the serviceâ??s security design; the key requirement is a tested independent recovery path. CSA authentication-method guide.

What if my phone is lost?

Use the platform or service recovery route and revoke credentials associated with the lost device. CSA MFA-bypass advisory.

Accuracy note: This article was checked against the linked primary sources on 2026-07-21. Individual facts and live services can change. No interview, first-hand use, first-hand meal, price check or field observation is claimed unless expressly stated.

Date Created
22/07/2026
Author

vanessakoh