

In today's digital landscape, users expect seamless access to their accounts across devices while maintaining strong security. However, account recovery is often an afterthought—addressed only during a frustrating lockout or security incident. Encouraging users to prepare recovery options ahead of time should be a priority for businesses serious about long-term digital identity management.

Industry leaders like **Arena Plus**, **Houzz**, and **Houzz Pro** have been innovating in this space by integrating passwordless access methods and security education nudges into their onboarding flows. This post walks through strategies to promote recovery preparedness that go beyond login and traditional password resets.

Understanding the Digital Identity Lifecycle Beyond Login

Most digital identity discussions focus on first-time login or sign-up. But the identity lifecycle extends much further, encompassing:

- Initial account creation with minimal friction
- Passwordless or biometric authentication options for everyday access
- Risk-based authentication and adaptive step-up verification for sensitive actions
- Recovery methods and backup setups for emergencies

Users often stall or skip over recovery setup, viewing it as unnecessary until faced with access issues. This gap puts both users and platforms at risk—users face lockouts, and businesses endure costly support tickets and potential reputational damage.

Keep Registration Simple and Clear

A foundational step toward encouraging backup method setup lies in the initial registration flow. Businesses like **Houzz** and its professional services arm **Houzz Pro** understand the importance of

- Clear, minimal registration fields
- Uncluttered screens free from optional permissions preselected
- Simple language that avoids jargon

This simplicity boosts conversion rates and yet provides the right setup cues for recovery without overwhelming users. For example: instead of asking for multiple optional contacts upfront, platforms can gently guide users later with nudges about recovery methods after account creation.

Example Minimal Registration Approach

Field	Purpose	Notes
Email or phone number	Primary identifier for login and communication	Only one required to keep friction low
Password or passkey setup	Secure authentication	Offer passwordless options for better security and usability
Recovery option prompt (optional at this stage)	Introduce importance of backup methods	Use educational microcopy to set expectations

Notice that the full backup method routine isn't forced here but set up to be introduced with contextual urgency later.

Promote Passwordless Access with Passkeys and Fingerprint Authentication

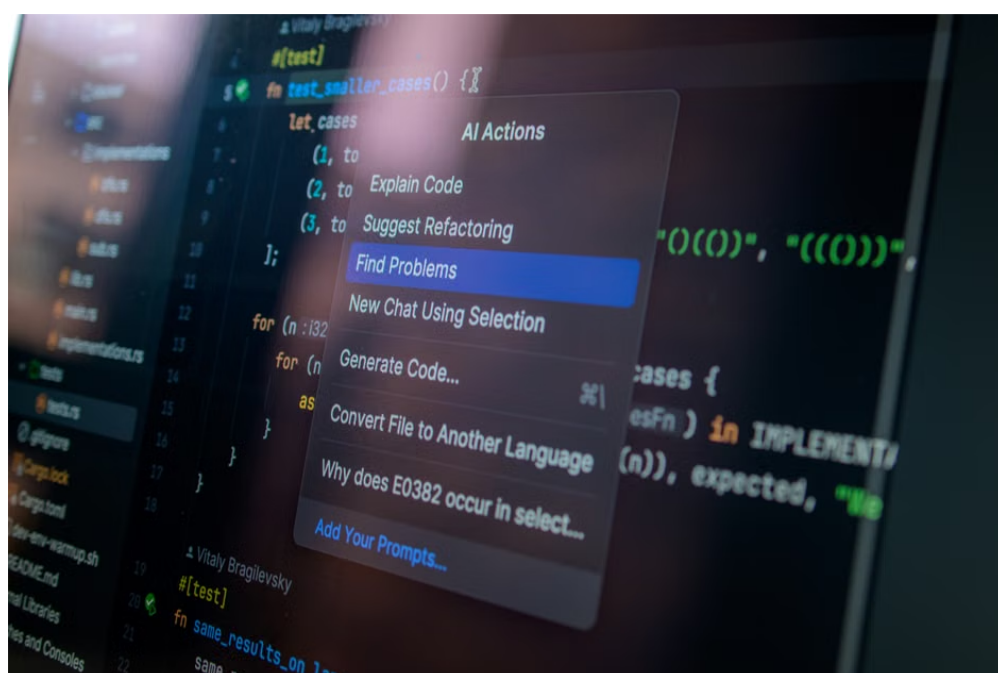
Empowering users to ditch passwords in favor of passwordless methods has multiple benefits:

- Eliminates weak or reused passwords
- Reduces phishing and credential stuffing risks
- Streamlines login with biometric options like fingerprint authentication

Passkeys are a powerful tool in this space. They use public-key cryptography secured on devices and biometrics, such as fingerprint sensors, allowing users to authenticate without entering anything to remember.

Arena Plus recently integrated passkey support in its mobile app, enabling users to authenticate via fingerprint or face recognition. This not only improved login success rates but also boosted users' trust by providing a familiar and secure access method.

By promoting biometric login and passkeys, companies can also better motivate users to add recovery methods. When users understand their accounts are tied to high-security tech, they recognize the need for thoughtful backups—such as provisioning secondary biometrics or trusted [one-time code via SMS](#) device lists.



Use Preparedness Nudges to Encourage Backup Method Setup

Nudges are subtle prompts designed to encourage users to take beneficial actions without pressure. They have proven effective in backup method setup by fostering security awareness and making recovery education part of normal flow.

Examples of *preparedness nudges* include:

- **Post-login reminders:** After successful sign-in, show a non-intrusive prompt: "For faster recovery during emergencies, set up a backup phone number or email."
- **Risk-based triggers:** If a login occurs from a new device or location, prompt the user to verify recovery details.
- **Contextual walkthroughs:** When users enable fingerprint authentication, display a quick tip on adding another biometric or device as an alternative recovery method.

Houzz Pro incorporates such nudges into their account settings, coupling each prompt with understandable explanations. This educates users on the benefits and reassures them about privacy and data safety.

Leverage Risk-Based Authentication and Step-Up Checks

Risk-based authentication systems assess the context of each authentication event to decide if additional verification is needed. Step-up checks might require:



- One-time passcodes to a trusted email or phone
- Biometric verification beyond the default method
- Answering personal security questions (used sparingly)

Here's why this is relevant for recovery:

- If users have already set up multiple recovery options, step-up is smooth and secure.
- Risk-based systems can highlight gaps in user recovery readiness, triggering timely nudges.
- This adaptive security method reduces friction for legitimate users while heightening protection against unauthorized access.

Products like Arena Plus leverage these tools to help users maintain confidence in their account security, promoting recovery setup as part of a holistic security approach rather than an isolated task.

Support Should Never Ask for These Recovery Details

It's important to reinforce to users what legitimate support channels will never ask for, building trust and preventing social engineering attacks. Keep a clear list visible in education emails or help articles, for example:

- **Never share your password or passkey with support agents.**
- **Support will never ask for the full contents of your recovery codes.**
- **Do not provide verification codes sent to you to anyone.**

This transparency and clarity boost user confidence and complement education nudges around backup method setup.

Conclusion

Encouraging users to set up recovery options before emergencies arise is an essential facet of managing the digital identity lifecycle. Companies like Arena Plus, Houzz, and Houzz Pro demonstrate that focusing on clear registration, passwordless access options such as passkeys and fingerprint authentication, preparedness nudges, and risk-based authentication can make recovery setups feel manageable and valuable.

By introducing backup method setup as a natural part of the user journey—backed by constant education and respect for privacy—platforms can reduce lockouts, improve security, and ultimately deliver a better user experience.