Phishing remains one of the most insidious threats to digital security. Despite ongoing efforts, attackers continue to exploit traditional authentication methods — especially SMS-based verification codes — to compromise accounts and steal identities. However, modern approaches to identity and access management offer more secure and user-friendly alternatives. In this post, we explore how companies like **Arena Plus**, **Houzz**, and **Houzz Pro** are enhancing security through passwordless technologies, risk-based authentication, and streamlined digital identity lifecycles that extend well beyond login.

The Problem with SMS Codes in Phishing Prevention

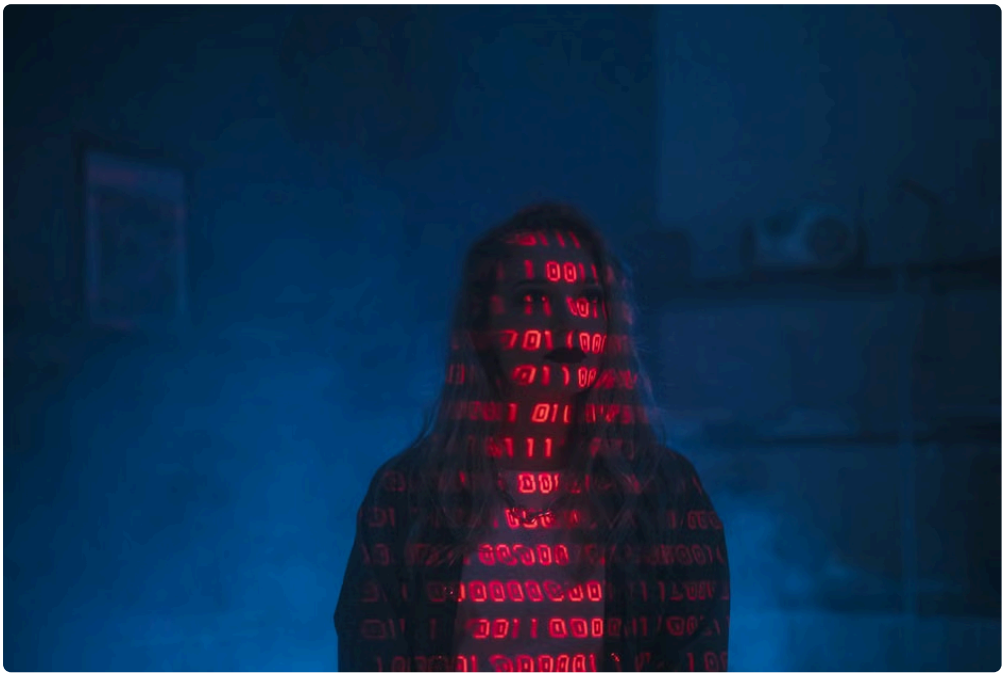
SMS codes have long been a popular secondary authentication factor, sent as text messages to users' phones during login attempts or sensitive operations. While SMS-based 2FA (two-factor authentication) adds a layer of security beyond passwords, it is not foolproof:

- **SIM swapping:** Attackers can hijack phone numbers by tricking mobile providers, intercepting SMS codes.
- **Phishing scams:** Fraudsters craft convincing messages prompting users to reveal SMS codes.
- **Message interception:** SMS messages can be intercepted or redirected by malware or network attacks.
- **User friction:** Receiving SMS codes adds delays and friction, increasing the chance of abandonment.

Given these risks and limitations, forward-thinking companies are shifting away from SMS reliance, focusing on more secure and seamless authentication methods.

Embracing a Digital Identity Lifecycle Beyond Login

Modern identity security isn't just about locking down the login screen — it's about managing a digital identity holistically throughout its lifecycle. Companies like **Arena Plus**, **Houzz**, and **Houzz Pro** illustrate this approach by integrating security at each stage:



1. **Clear, minimal registration:** Reducing friction while collecting only essential data.
2. **Passwordless authentication:** Using technologies like passkeys and fingerprint authentication.
3. **Risk-based monitoring:** Continuously evaluating activity and applying step-up authentication when needed.

4. **Account recovery and session management:** Ensuring smooth yet secure paths for regaining access or ending sessions.

This lifecycle perspective strengthens security, reduces phishing windows, and delivers better user experiences.

Clear, Minimal Registration Fields to Build Trust and Security

One early mistake in identity management is overwhelming users with complex registration forms. Long lists of fields can deter sign-ups and cause users to input inaccurate information. Additionally, inconsistent terminology between registration and recovery processes only adds confusion and support load.

Leading platforms focus on:

- **Essential data only:** Requesting the bare minimum to identify and authenticate users.
- **Consistent labels:** Using uniform terminology across registration, login, and recovery screens.
- **Real-time guidance:** Clearly indicating requirements upfront to prevent errors.
- **Opt-in permissions:** Ensuring no permissions or marketing consents are preselected.

These design choices not only improve user satisfaction but also reduce security risks associated with inaccurate or incomplete identity data.

Passwordless Access: Leveraging Passkeys and Fingerprint Authentication

The heart of reducing phishing risk lies in eliminating shared secrets like passwords and SMS codes. **Passkeys**, supported natively on many devices, enable passwordless authentication by securely storing cryptographic credentials that never leave the device.

Fingerprint authentication — a biometric method — further strengthens this approach by requiring a physical factor unique to the user.

Here's how the combination works:

- **Passkeys:** When registering, the user's device creates a public-private key pair. The private key remains on the device, while the public key is stored server-side.
- **Authentication:** At login, the device proves possession of the private key, often gated by fingerprint authentication.
- **Phishing resistance:** Since no passwords or codes are transmitted or stored centrally, attackers can't intercept or reuse credentials.

Arena Plus and **Houzz Pro** have started integrating passkey support into their apps, providing their users seamless, passwordless, and highly secure access.

In-App Messages and Short-Lived Links: Secure Communication Channels

When notifications or sensitive operations require user attention, SMS codes have traditionally been used. However, modern alternatives use secure **in-app messages** and **short-lived links** to reduce phishing attack surfaces.

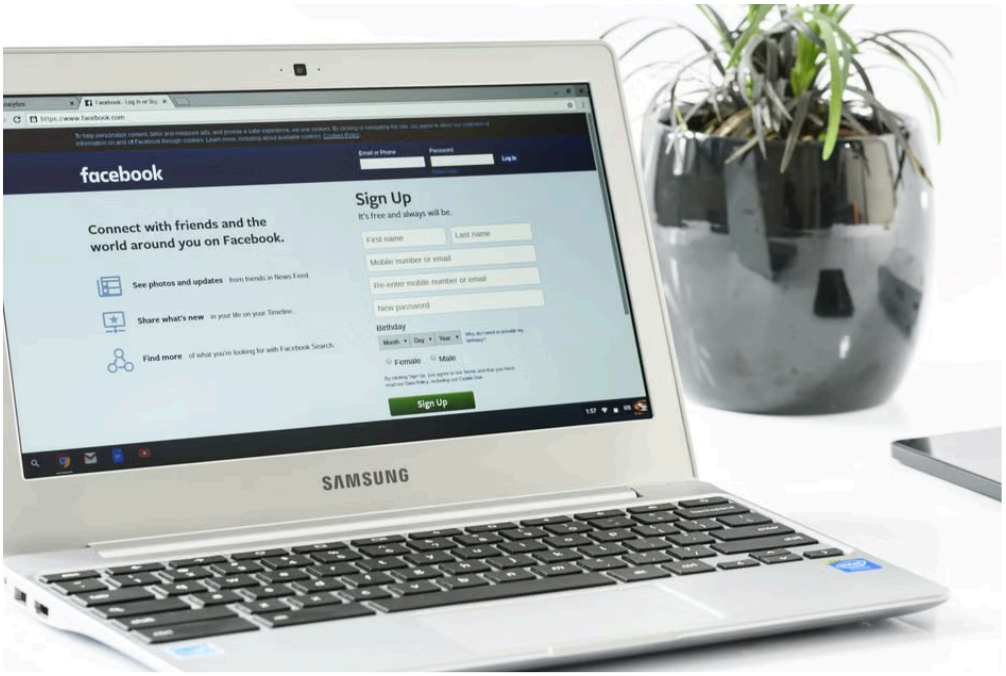
- **In-app messages:** Displayed securely within the authenticated app environment, these messages avoid the vulnerabilities inherent in SMS.

- **Short-lived links:** Sent via email or in-app notifications, these links provide time-limited access to sensitive functions, like updating profiles or confirming transactions.

By implementing these channels, platforms like **Houzz** improve security without sacrificing convenience or user trust.

Risk-Based Authentication and Step-Up Checks

Let me tell you about a situation I encountered wished they had known this beforehand.. Even with strong passwordless methods, some transactions or circumstances require additional verification. Risk-based authentication dynamically assesses factors Take a look at the site here such as:



- Device reputation
- Location anomalies
- Behavioral deviations

You ever wonder why if the system detects suspicious activity, it applies step-up checks such as biometric re-authentication or a push notification prompt.

For example, **Arena Plus** employs adaptive risk models to balance security and user convenience, demanding additional proof only when needed, substantially lowering false rejections and phishing vulnerability.

Best Practices Summary: Reducing Phishing Beyond SMS Codes

Strategy Description Benefits Clear, minimal registration Collect only necessary user info with consistent terminology Reduces errors and user friction; improves data accuracy Passwordless access with passkeys & fingerprint Use device-stored keys with biometric gating for login Eliminates shared secrets prone to phishing or theft In-app messages and short-lived links Communicate sensitive actions within secure channels Prevents interception and redirection risks of SMS Risk-based authentication and step-up checks Adaptively require additional verification based on risk Provides layered security without burdening all users

Conclusion

Phishing will always be a threat, but relying on SMS codes as a frontline defense is no longer adequate. By adopting a full digital identity lifecycle strategy — from simple, clear registration through passwordless passkey authentication and dynamic, risk-aware step-up verifications — companies like **Arena Plus**, **Houzz**, and **Houzz Pro** are setting new security standards.

Key to success is embracing modern tools that users already trust on their devices, such as fingerprint authentication and in-app messaging, while avoiding outdated approaches that invite phishing vulnerabilities. These methods not only strengthen security posture against attackers but also deliver a more seamless and respectful user experience.

Secure your digital identity the smart way: move beyond SMS codes and into a future of phishing-resistant authentication today.