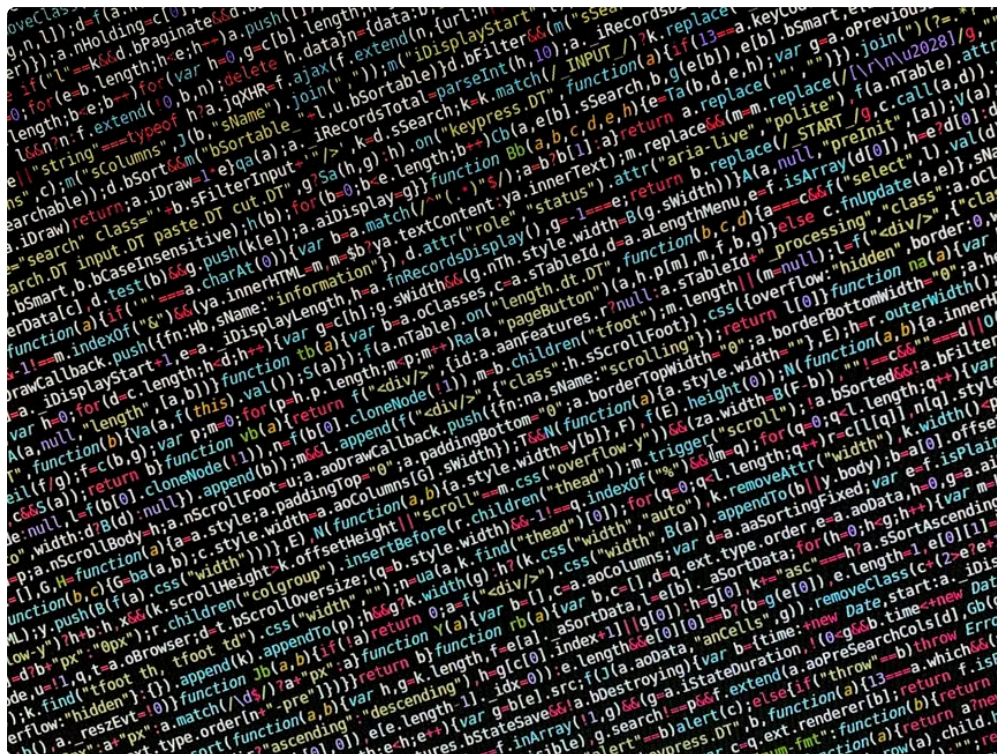


In today's interconnected world, managing the devices authorized to access your accounts is more important than ever. Whether you're using services from Arena Plus, Houzz, or Houzz Pro, keeping track of where and how your account is accessed helps protect your digital identity beyond the initial login. A well-designed device management page empowers users to **remove devices**, review their **authorized devices list**, and **report suspicious activity** with ease.

Why Device Management Is Part of the Digital Identity Lifecycle

Most digital security efforts focus on login and registration — but identity management extends well beyond those first steps. The digital identity lifecycle includes:



- **Device Authorization:** Recognizing which devices are trusted.
- **Ongoing Monitoring:** Watching for unusual activity from known or unknown devices.
- **Risk-Based Authentication:** Applying extra verification steps only when needed.
- **Account Recovery:** Regaining access securely when devices are lost or stolen.

Services like Arena Plus and Houzz Pro are already embracing passwordless access methods such as **passkeys** and biometric options like **fingerprint authentication**. Combining these modern authentications with <https://www.gardenweb.com/hznb/projects/arena-plus-and-the-future-of-trusted-digital-identity-pj-vj~7901764> a clear device management interface enhances security and reduces user friction.

Key Principles for Building a Device Management Page Users Understand

When designing a device management page, clarity and functionality are paramount. Users should confidently find their authorized devices, know how to remove devices they no longer use, and report suspicious activity without confusion. Here are essential principles to follow:

1. Clear and Minimal Registration Fields Reduce Friction

Start by minimizing the complexity users face during the registration and login process. Avoid asking for unnecessary information. Many users abandon forms when fields seem redundant or overly complicated. For example, Arena Plus's streamlined registration process features minimal fields that prioritize only essential data.

Consistency matters: the terminology used during registration must match what users see later in device management. Avoid switching between terms like "trusted devices" and "authorized devices"—choose one and stick with it to avoid confusion.

2. Present an Intuitive Authorized Devices List

Your device list should answer simple questions at a glance:

- Which devices currently have access?
- When was each device last used?
- What kind of device is it? (e.g., smartphone, laptop, tablet)
- Where was it last used? (location or IP address, presented simply)

Avoid showing unreadable browser strings. Instead, detect and display known device types and OS details, as Houzz effectively does. Use recognizable device names or allow users to label devices themselves.

3. Provide Easy Options to Remove Device Access

Users need a clear, prominent "Remove Device" button or link for every device, especially for lost or outdated hardware. The removal action should have a simple confirmation step to prevent accidental removal, but avoid overly complex CAPTCHA or multi-step pop-ups that disrupt flow.

Explain in plain language what happens when a device is removed. For instance: " *Removing this device will require logging in again if you want to use it.*" This transparency reassures users about consequences.

4. Encourage Reporting Suspicious Activity Effectively

If users notice unusual devices or behavior, they must quickly report this without guessing. Avoid vague alerts like "Unusual activity detected" — instead, use clear, non-alarming messages that describe the problem plainly.

Include a straightforward "Report Suspicious Activity" button or link near the device list. When tapped, provide a simple form to flag the issue and instructions on next steps. Support communications generated from these reports should clearly state:

- What the user should NEVER share (e.g., passwords, full credit card numbers).
- How support will respond and protect user privacy.

5. Integrate Risk-Based Authentication and Step-Up Checks

Not all login attempts require the same level of scrutiny. Use risk-based authentication to selectively require stronger verification methods when a new or unusual device accesses an account. For example, if a user logs in from a new smartphone, prompt for **fingerprint authentication** or a passkey verification.

This approach balances security with user convenience, something Houzz Pro integrates to allow trusted devices seamless access while securing new device attempts.

Design Considerations: Lessons from Leading Services

Arena Plus: Simplicity and Security

Arena Plus emphasizes minimal data entry and seamless passwordless experiences. Their device management pages emphasize readability, with device types labeled clearly and easy removal options presented upfront. If suspicious activity is detected, Arena Plus clarifies the exact nature of the concern and the user's options, choosing clear language to avoid user fear.

Houzz and Houzz Pro: Professional-Grade Controls

Houzz and Houzz Pro users often manage multiple projects and devices. They benefit from a device management portal that supports multiple authorized devices with customized labels, easy removal, and up-to-date device information that goes beyond generic browser strings.

Houzz Pro also leverages biometric options like fingerprint authentication for easier and more secure step-up verification, demonstrating the importance of integrating strong authentication with device management.

Implementing Passwordless Access with Passkeys

Traditional passwords are a weak link in security. Passkeys provide a secure, phishing-resistant alternative that pairs well with device management. Since passkeys are stored securely on each authorized device, removing a device from the authorized list instantly revokes access from that device.

When building your device management page, clearly show users which devices have active passkeys and which might require re-registration after removal or reset. This transparency helps users manage their security confidently.

Security and Privacy Best Practices

- **Avoid Displaying Sensitive Information:** Never show full IP addresses or precise locations. General geographic regions are safer and sufficient.
- **Notify on Changes:** Send email or push notifications when devices are added or removed to keep users informed.
- **Stay Consistent:** Use uniform terminology like "Authorized Devices" throughout the user journey.
- **Make Support Transparent:** Include an explicit message: "Support will never ask for your password or full payment details." Keep a running list of what support teams should never request.
- **Don't Premake Optional Permissions:** Let users actively enable biometric or passkey authentication rather than having these preselected.

Summary

Creating a device management page that users truly understand requires simplicity, clarity, and integration with modern security tools. By focusing on a clean **authorized devices list**, intuitive controls to **remove devices**, and easy methods to **report suspicious activity**, companies like Arena Plus, Houzz, and Houzz Pro set a high standard. Incorporating **passkeys**, **fingerprint authentication**, and **risk-based step-up checks** strengthens security without frustrating users.



Remember, device management is a vital part of the ongoing digital identity lifecycle. By building systems that are both secure and user-friendly, you help people keep their accounts safe and their digital lives worry-free.