

Daily UI #006

Privacy & Security Settings — Deep UX/UI Case Study

CreateHub — a mobile settings experience designed to give users clear, understandable control over account security, privacy and personal data.

01 — Challenge Brief

Prompt: Design settings for something such as security, privacy, game settings, appearance or system controls.

Objective: Create a settings experience where users can quickly find important controls, understand what each option does and change sensitive settings confidently.

02 — Product & Platform

Product: CreateHub, a creative community for designers, illustrators, developers and creators.

Platform: Mobile app — 390 × 844 px.

The mobile-first approach focuses on scanability, touch-friendly controls, clear grouping and safe interaction patterns.

03 — Selected Setting Type

Instead of designing a generic list of app settings, this challenge focuses on **Privacy & Security**. These settings are high-value because they affect account protection, visibility, communication and personal data.

04 — Target User

Riya Sharma, 26 — Product Designer.

Goal: Control who can access her account and interact with her.

Needs: Clear explanations, visible setting states, secure account controls and easy recovery from mistakes.

Frustrations: Technical language, hidden controls and uncertainty about what changing a setting will do.

05 — Problem Definition

Security settings can become overwhelming when users see technical terms, too many options or unclear consequences. A good settings experience should make the current state obvious and explain important consequences before users commit to a change.

How might we give users meaningful control over privacy and security without making the settings experience complicated?

06 — User Goal

“I want to easily understand and control who can access my account and interact with me.”

07 — UX Principle

Explain first → Show current state → Let users control → Confirm sensitive actions.

08 — Information Architecture

Group	Important settings
Account Security	Change Password, Two-Factor Authentication, Login & Active Sessions, Security Alerts

Privacy & Visibility	Profile Visibility, Message Permissions, Activity Status, Blocked Accounts
Data & Privacy	Download My Data, Data & Privacy Policy
Everyday Preferences	Notifications, Appearance, Language, Help & Support
Danger Zone	Delete Account

09 — User Flow

Open Settings → Review account security → Open Privacy & Security → Choose a setting → Understand current state → Change setting → Confirm if sensitive → Receive feedback

10 — Main Settings

Account Security: Change Password, Two-Factor Authentication, Login & Active Sessions, Security Alerts.

Privacy: Profile Visibility, Message Permissions, Activity Status, Blocked Accounts.

Data: Download My Data and Data & Privacy Policy.

Danger Zone: Delete Account.

11 — Settings Grouping Strategy

Related controls are grouped so users do not have to scan one long list. High-risk actions are separated from everyday preferences. Descriptions are used for settings where the label alone may not explain the consequence.

12 — Privacy Visibility Experience

The Profile Visibility screen offers three clear options: **Public**, **Followers Only** and **Private**. Each option includes a short explanation of who can see the user's profile and content.

13 — Interaction Strategy

Simple reversible preferences can use switches. Choices with mutually exclusive options use radio controls.

Sensitive actions such as password changes, account deletion or security changes use confirmation and, when appropriate, identity verification.

14 — Wireframe Exploration

Variation 1 — List First: Traditional grouped settings list with simple rows.

Variation 2 — Security Dashboard: Strong security status card followed by privacy controls.

Variation 3 — Guided Settings: Security summary, grouped controls and deeper detail screens.

Selected: Variation 3 because it provides the strongest balance between quick scanning and detailed control.

15 — Visual Design Direction

Style: Clean + Minimal + Trustworthy.

Background: #F7F7FA **Surface:** #FFFFFF **Text:** #171717 **Primary:** #5B5CE2.

Positive/security: #16A34A **Destructive:** #DC2626.

Typography: Inter, with strong section headings, concise descriptions, rounded surfaces and restrained iconography.

16 — Security Status

The main Settings screen includes a lightweight security summary such as “**Your account is secure**” when key protections are enabled. This provides reassurance without turning the settings page into a technical security dashboard.

17 — Interaction States

State	Behavior
Default	Current settings are clearly visible.
Toggle On/Off	Immediate visual state change with confirmation where appropriate.
Radio Selection	Selected option is clearly indicated.
Sensitive Action	Confirmation or identity verification before changing.
Success	Short confirmation explains that the change was saved.
Error	Specific explanation plus a recovery action.
Loading	Skeleton or progress state preserves layout and context.

18 — Error & Recovery

Errors should explain what happened and what the user can do next. Example: **“We couldn’t update your privacy setting. Check your connection and try again.”** Sensitive changes should never silently fail.

19 — Destructive Actions

Delete Account is separated into a visually distinct danger zone. The action requires an explicit confirmation and should clearly explain permanence and relevant consequences. Destructive styling is reserved for genuinely irreversible actions.

20 — Accessibility

Use sufficient contrast, readable labels, meaningful icon descriptions, logical focus order, large touch targets and text alternatives for status. Do not communicate enabled/disabled states using color alone.

21 — Privacy & Safety Considerations

Privacy settings should default to understandable choices rather than hidden assumptions. Users should know what information is public, who can contact them, and which activity information may be visible. Sensitive account information should not be exposed unnecessarily.

22 — Responsive Thinking

The primary design is mobile-first. On larger screens, grouped settings can become a two-pane layout with categories on the left and details on the right while preserving the same hierarchy and interaction logic.

23 — Key Design Decisions

1. **Grouped settings:** reduces scanning effort.
2. **Security summary:** gives users immediate reassurance.
3. **Descriptive labels:** explains important consequences.
4. **Correct controls:** switches for toggles, radios for exclusive choices, navigation for deeper settings.
5. **Confirmation for sensitive actions:** prevents accidental changes.
6. **Danger zone separation:** keeps destructive actions away from everyday settings.
7. **Consistent states:** users always know whether a change succeeded.

24 — Success Criteria

A user should be able to find an important setting quickly, understand what it controls, see its current state, change it confidently and understand the consequences of sensitive actions.

25 — Final UI Review

The selected high-fidelity direction combines a personal Settings overview, account-security status, grouped Privacy & Security controls and a detailed Profile Visibility screen. The result feels modern and friendly while treating privacy and security as serious product responsibilities.

26 — Learnings

The key learning is that settings UX is not about listing every option. It is about **organization, clarity and safe control**. Users should never have to guess what a setting means, what state it is in, or what will happen after they change it.

Portfolio Takeaway

Daily UI #006 demonstrates information architecture, settings hierarchy, privacy UX, security flows, control selection, interaction states, error recovery, accessibility, responsive thinking and responsible handling of sensitive user controls.