Float Account Security 101

Essential Account Safety

These are general best practices that apply to Admins and Managers

60-Day Rule: if you notice any unauthorized activity on your Visa or Mastercard cards, it's important to report it within 60 days. After that, it gets tricky for Float to help out. Keep an eye on your transactions regularly and reach out to us.

Deleting Accounts: When an employee is being let go or is leaving - their Float account should be deactivated immediately to avoid surprise transactions.

Logins: Use secure devices and connections to log in to Float. We also offer MFA and SSO options (SSO on Pro)

Limit Admin Access: Admins have more functionality in the App. Be mindful of who is getting access.

Bookmark the login page: Avoid searching for Float on Google, as fake websites may appear. Instead, bookmark the official login link or access it through your password manager.

Important Add ons

Float offers a variety of features to help you protect your business

Merchant Controls: Limit where your employee's cards can be used, giving them only what they need

Submission Policies: Create custom rules so that cards are paused if your employees do not submit receipts

Notifications: Choose a notification setting (text, email, slack) that allows you to react quickly if you see any unrecognized transactions.

Other Considerations

Pro tips for extra protection

Card Limits: Assign the amount your employees need

Leaves: Consider pausing the cards of employees going on leave as they will not likely check in regularly

Re-Assigning Cards: Re-assigning cards is useful for maintaining subscriptions. However, if the card belongs to an employee who was let go or left on bad terms, the card should be terminated instead.