**Why Creating Individual IAM Accounts is Safe and Beneficial**

1. **Granular Access Control**: By creating individual IAM accounts, you can assign specific permissions to each user based on their role and responsibilities. This ensures that users have only the access they need to perform their tasks, following the principle of least privilege.
2. **Accountability and Auditing**: Individual accounts make it easier to track user activities. AWS CloudTrail logs actions performed by IAM users, which helps in auditing and identifying who did what.
3. **Security Best Practices**: Individual IAM accounts allow you to enforce security best practices such as multi-factor authentication (MFA), password policies, and access keys rotation for programmatic access.
4. **Revoking Access**: If an employee leaves the company or changes roles, you can easily revoke or adjust their access without affecting other users.

**Best Practices for Managing IAM Accounts**

1. **Use Groups to Assign Permissions**:
   * Create IAM groups based on job functions (e.g., "Lead Engineers," "Junior Engineers," "Interns," "Consultants").
   * Attach policies to these groups and add users to the appropriate groups. This makes managing permissions easier.
2. **Enable Multi-Factor Authentication (MFA)**:
   * Require MFA for all IAM users to add an extra layer of security.
3. **Use Strong Password Policies**:
   * Enforce strong password policies to ensure that IAM user passwords are secure.
4. **Rotate Credentials Regularly**:
   * Regularly rotate passwords and access keys for IAM users.
5. **Monitor and Audit IAM User Activities**:
   * Use AWS CloudTrail to monitor and audit IAM user activities.
   * Set up CloudWatch Alarms for specific activities that need attention.
6. **Apply the Principle of Least Privilege**:
   * Grant the minimum permissions necessary for users to perform their job functions.
   * Regularly review and adjust permissions as needed.

**Step-by-Step Guide to Creating IAM Users and Groups**

**Step 1: Create IAM Groups**

1. **Navigate to IAM**:
   * Sign in to the AWS Management Console and go to the "IAM" service.
2. **Create Groups**:
   * Click on "User groups" in the left-hand menu.
   * Click "Create group."
   * Name the group based on the role (e.g., "Lead Engineers," "Junior Engineers," "Interns," "Consultants").
   * Attach the appropriate policies to the group.
   * Click "Create group."

**Step 2: Create IAM Users**

1. **Navigate to IAM**:
   * Click on "Users" in the left-hand menu.
   * Click "Add user."
2. **Add User Details**:
   * Enter the user name.
   * Enable "Programmatic access" and "AWS Management Console access" if needed.
   * Set a custom password or allow the system to generate one.
3. **Assign User to Groups**:
   * On the "Set permissions" page, add the user to the appropriate group created earlier.
   * Click "Next: Tags" (optional to add tags).
   * Click "Next: Review" and then "Create user."
4. **Repeat for All Users**:
   * Repeat the process for all engineers and interns.

**Summary**

1. **Create IAM Groups**:
   * Create groups based on job functions and attach appropriate policies.
2. **Create IAM Users**:
   * Create individual IAM users for each engineer and intern.
   * Assign users to the appropriate groups to inherit permissions.
3. **Implement Best Practices**:
   * Use MFA, strong password policies, regular credential rotation, and monitoring to ensure security.

By following these steps and best practices, you can safely and effectively manage access for your engineers and interns using IAM accounts. This approach ensures security, accountability, and ease of management.