

Social media security checklist

Protect your brand and reputation with these essential steps for securely managing access to your business's social media accounts.



- 1. Inventory all organic and paid social media accounts** ☐
Create a list of all your company's social media accounts. A quick trick? Google your brand and platform names (e.g., "Instagram Acme Corp") to catch any accounts that may have slipped through.
- 2. Review third-party app access** ☐
Regularly check each account's settings (usually under security > apps & sessions) to review third-party apps and permissions. If an app is no longer used or permissions aren't necessary, revoke access immediately.
- 3. Deactivate inactive or unused accounts** ☐
Review which accounts are still part of your social strategy. Deactivate any that are no longer relevant or active, and audit for ghost accounts that could be lingering unnoticed.
- 4. Use unique, corporate email addresses** ☐
Avoid personal emails and profiles, and make sure each address is tied to your company domain for better control and security.
- 5. Set strong passwords and update them regularly** ☐
Create unique, complex passwords for each account using a password manager. Never reuse passwords across accounts, and don't share them. Updated passwords regularly.
- 6. Turn on the strongest form of Multi-Factor Authentication (MFA)** ☐
Enable MFA for all social media accounts—no exceptions. Link MFA to corporate emails or authenticator apps, avoiding personal emails and phone numbers for security and team productivity reasons.
- 7. Monitor ad spend** ☐
Set up a routine to review ad spending on platforms like Meta and LinkedIn. Compare it to normal patterns to catch any unusual spikes or redirections, indicating unauthorized activity.
- 8. Review and restrict user access** ☐
Establish a regular schedule to review and adjust access. Apply the 'least privilege' approach, granting only the access necessary and removing users who no longer need it.
- 9. Implement an offboarding process for employees, freelancers, and agencies** ☐
Develop a clear and immediate offboarding process to remove access for users as soon as they leave the company, team, or project—no delays.
- 10. Strengthen collaboration across Marketing, IT, and Security** ☐
Ensure strong communication between IT, Security, and Marketing to manage access to corporate social media accounts, implementing best practices and adopting solutions that strengthen security without friction or manual effort.

About Cerby

Cerby provides Marketing and IT teams with the only solution for securely and centrally managing access across all social media platforms. We automate and simplify key identity processes, including password rotations, MFA enforcement, managing user access, onboarding & offboarding agencies and freelancers, and monitoring shared accounts. By streamlining these tasks, Cerby enhances team productivity, enables seamless collaboration with external parties, and safeguards your brand's online presence, allowing your teams to focus on growth without worrying about social media security.

Visit us at [Cerby.com](https://cerby.com) and follow us on social at [@CerbyHQ](https://twitter.com/CerbyHQ).