

Social Media Cybersecurity Audit Checklist

Completed	Action Item	Description	Assignee
	Use secure platforms	Confirm your chosen CMS and publishing tools use strong security standards, regularly update their systems, and support MFA.	
	Enable MFA and update passwords	Require MFA on all marketing and social platforms. Rotate passwords quarterly.	
	Limit admin access	Restrict admin roles to essential personnel. Audit permissions monthly.	
	Vet third-party tools/plugins	Confirm chosen extensions/tools use strong security records and active maintenance systems and platforms. Contact extensions/tools' customer service to confirm, if needed.	
	Keep software and plugins updated	Ensure all plugins, CMS tools, and browser extensions are updated regularly.	
	Audit email/automation tools	Create a routine to rotate API keys and limit tool integrations. Monitor for suspicious activity.	
	Stay alert for phishing	Train team members to spot fake collabs, credential scams, and suspicious links.	
	Train your team	Run quarterly cybersecurity training and awareness drills.	
	Monitor accounts for suspicious activity	Set up account monitoring and alerts. Check logs weekly.	
	Encrypt data & ensure privacy compliance	Encrypt data at rest and in transit. Follow GDPR, CCPA, and other applicable standards.	
	Include cybersecurity in campaign planning	Identify potential vulnerabilities in creative concepts and activation plans.	
	Build an incident response plan	Define roles and recovery steps for social account compromise or data loss.	