Cyber Security for Creative Agencies (UK)

Protect your creative projects, client data and cloud accounts with confidence.

You rely on tools like Adobe, Google Workspace, Microsoft 365, Canva, Figma, WordPress, HubSpot, Dropbox and Slack every day. But every shared password, open drive, or unchecked email adds unnecessary risk.

Strengthening your cyber security doesn't have to slow you down - it helps protect your reputation, your work and your clients.

This checklist helps you build stronger security across your agency while keeping creativity flowing.

1 Access & Authentication

- [ ] Each team member has their own login - no shared email or admin accounts
- [ ] Multi-Factor Authentication (MFA) is turned on for all cloud and email accounts
- [ ] Freelancers and contractors have limited access and are removed when projects end
- [ ] Passwords are unique and never reused across systems
- [ ] All passwords or passphrases are strong (at least 12 characters or three random words)
- [ ] A password manager (e.g. Keeper) stores shared credentials securely
- [ ] Account lockout triggers after multiple failed attempts
- [ ] Password resets follow a secure identity verification process

💡 **Quick win:** *Shared logins are the number one cause of agency data leaks. Make MFA and unique accounts mandatory.*

2 Your Email & Brand Reputation

- [ ] Email accounts are protected by phishing and impersonation filtering
- [ ] DMARC, SPF and DKIM are correctly set up on your domain
- [ ] Your team knows how to spot fake client or invoice emails
- [ ] You use clear email signatures and verification steps for sensitive messages
- [ ] No one sends client passwords or documents via unsecured email

💡 **Quick win:** *Set up DMARC, SPF and DKIM correctly to stop attackers spoofing your domain. Add phishing and impersonation filters to protect your team and clients.*

3 Your Devices

- [ ] All laptops and desktops are password-protected and encrypted
- [ ] Devices lock automatically after a few minutes of inactivity
- [ ] Only authorised staff use company devices for client work
- [ ] Devices are updated and patched automatically
- [ ] Mobile phones used for client accounts or social platforms have MFA enabled

💡 **Quick win:** *A lost laptop without encryption can expose every client you've ever worked with.*

4 Your Cloud Tools

- [ ] Only approved staff have access to cloud tools (Google Drive, Dropbox, Canva, Figma, etc.)
- [ ] Old folders, projects and client drives are reviewed and access removed regularly
- [ ] MFA is enabled on every cloud account
- [ ] Shared drives and folders are restricted by permissions — not open links
- [ ] Personal accounts are never used for client work

💡 **Quick win:** *"Anyone with the link" sharing is one of the biggest cloud security risks.*

5 Your Creative Assets & Projects

- [ ] Project files and assets are backed up automatically
- [ ] You can recover deleted or overwritten files quickly
- [ ] Large transfers (e.g. video, design files) use secure transfer tools, not public links
- [ ] All client work is stored on agency-approved platforms
- [ ] Offline copies of assets are encrypted and stored securely

💡 **Quick win:** *If a freelancer deletes or loses files, you should be able to recover them within minutes.*

6 Your Freelancers & Contractors

- [ ] Each freelancer has a unique login or secure invitation
- [ ] Access is time-limited and removed after projects finish
- [ ] Freelancers use MFA and follow safe password practices
- [ ] Master passwords or client credentials are never shared over email or chat

💡 **Quick win:** *Give every contractor their own login, limit access by project and remove it when the work ends.*

7 Your Social & Client Platforms

- [ ] MFA is enabled on Meta, LinkedIn, Google Ads and all client platforms
- [ ] Admin access is restricted to trusted team members
- [ ] A shared password manager is used for login management
- [ ] Client accounts are not linked to personal profiles
- [ ] You maintain an up-to-date record of who has access to each platform

💡 **Quick win:** *Enable MFA on all social and client marketing platforms to stop account takeovers.*

8 Your Backups & Recovery

- [ ] Files and assets are backed up daily or automatically
- [ ] Cloud data (Google Drive, OneDrive, etc.) is protected by a backup service
- [ ] Backup restores are tested periodically
- [ ] Backups are separate from production accounts
- [ ] You know how long it would take to restore key data

💡 **Quick win:** *Set up automated cloud backup so deleted or changed files can always be recovered.*

9 Your Awareness & Culture

- [ ] Your team knows how to report suspicious emails or incidents
- [ ] You run regular phishing awareness training
- [ ] New starters receive a short cyber induction
- [ ] Security isn't blamed — it's part of your creative culture
- [ ] You review security quarterly with your IT or cyber provider

💡 **Quick win:** *Most cyber issues come from habits, not hackers. Build security into everyday conversations.*

Who this is for

This checklist is designed for:

- Marketing, design and branding agencies
- Digital studios and freelancers handling client data
- PR, content and social media teams
- Video, animation and production houses
- Web designers, developers and WordPress specialists
- Any creative business using cloud platforms like Adobe, Canva, Google Workspace or Microsoft 365

If you manage client accounts, brand assets or creative projects online, this guide helps you strengthen your cyber security without slowing down your creative flow.

Quick Wins for Creative Teams

- [ ] Turn on MFA for all logins
- [ ] Check your DMARC report
- [ ] Store all credentials in a password manager
- [ ] Review who has access to client drives
- [ ] Back up all your project files
- [ ] Review freelancer and contractor permissions
- [ ] Encrypt every device that holds client data

BLACK SWAN
CYBER SECURITY SOLUTIONS

Need help securing your agency?

We help marketing, design and creative agencies protect their client work, brand reputation and cloud systems - without disrupting creativity or collaboration.

blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142