CyberWardens.

FACTSHEET

Social media safety for small businesses

Secure the social media accounts your business relies on

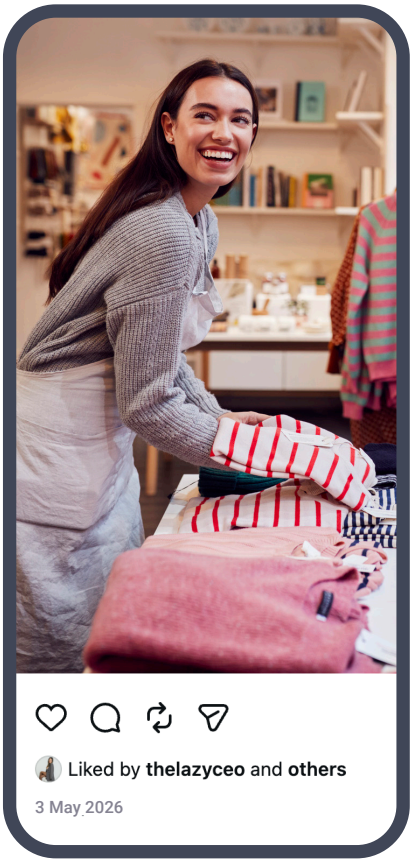
Social media helps small businesses reach customers, build trust and grow their brand. But platforms like Facebook, Instagram, LinkedIn and TikTok are also attractive targets for cyber criminals looking for a way into your business, your ad accounts and your customer relationships.

A hacked account can quickly become a public, costly and stressful incident. Cyber criminals may lock you out, post harmful content, run scam ads using your credit card, impersonate your business or target your customers under your name.

These attacks can cause financial damage, reputational harm and take weeks, months, or even years, to recover from. Some small businesses never will.

Luckily, there are some simple ways you can lock the door of your virtual shopfront and get back to posting about your upcoming flash sale, pop-up store or 'behind-the-scenes' reel with confidence.

To help, we have developed this fact sheet that shares practical steps to protect your business accounts, spot common social media scams and separate personal and business access so one hacked login does not put your whole business at risk.



CyberWardens.

Why social media is a lucrative target

For many small businesses, social media accounts are linked to credit card details, advertising budgets, customer, client or patient data, booking enquiries, brand assets and sometimes sensitive business information.

That makes them valuable targets for hackers, who can gain access through phishing messages, stolen passwords, or unsecured devices. Once inside, they can impersonate your business, steal funds, run malicious ads, scam your customers, harvest data or lock you out entirely.

And because platforms such as Facebook or Instagram are often your most visible business channels, the reputational damage can be swift and public.

Cyber criminals don't discriminate based on business size.

According to the Australian Cyber Security Centre (ACSC), 43% of cyber crime targets small businesses. They are targeted because attackers know there is usually no dedicated IT support and limited time to respond to incidents.

Attackers see them as easy targets with weak security and a higher chance of paying ransoms, or a stepping stone to larger business partners.

Social media scams to look out for

Fake platform support messages: Messages or emails pretending to be from Facebook, Instagram, TikTok or LinkedIn. They may claim your account will be banned, your ads have breached a policy, or your page needs urgent verification. The link usually leads to a fake login page designed to steal your details.

Phishing and suspicious links: Attackers send fake prize offers, collaboration requests, copyright warnings, customer complaints or direct messages to trick you into clicking a link or sharing login details.

Account hijacking and impersonation: Criminals take over your account, or create a fake profile or duplicate page pretending to be your business, to scam customers, damage your reputation or harvest followers and data.

Compromised ad accounts: Business accounts often store credit card details for advertising. Criminals may use those accounts to run scam ads, cryptocurrency promotions, fake giveaways or harmful content paid for by you.

Fake suppliers and marketplace scams: Fake social media pages and ads may promote products, services or business supplies that never arrive, or direct customers to scam websites.

Malware: A fake collaboration brief, invoice, image file or ad link may install malicious software on a device. This can allow criminals to steal login details or access business accounts.

AI impersonation and deepfakes: Criminals can use artificial intelligence to create fake endorsements, voice clips or videos that appear to feature business owners, staff, customers or public figures.

Quick check

- ✔ Be suspicious of urgent messages asking you to 'verify', 'appeal', 'restore access' or 'avoid suspension'.
- ✔ Do not log in through a link sent by email, direct message or text. Open the platform directly in your browser or app.
- ✔ Check the sender, URL and wording carefully. Scam messages often use pressure, threats or offers that feel too good to be true.
- ✔ If you manage ads, check your ad spend and payment activity regularly for unusual spikes or campaigns you did not create.

CyberWardens.

How to protect your social media accounts

Use strong, unique passphrases: Use a different long passphrase for every business account. A passphrase made from four or more random words is easier to remember and harder to guess than a short password.

Use a password manager: Store business passphrases in a reputable password manager, rather than saving them in browsers, spreadsheets, notes apps or shared documents.

Turn on multi-factor authentication: Enable MFA or two-step verification for every social media, email and ad account. Where possible, use an authenticator app rather than SMS.

Secure the email account linked to your socials: Your email is often the key to resetting social media passwords. Protect it with a strong passphrase, MFA and current recovery details.

Review admin access: Only give admin access to people who need it. Use platform roles or business tools instead of sharing passwords, and remove access when staff, contractors or agencies leave.

Check logged-in devices: Regularly review where your accounts are logged in. Remove unfamiliar devices and sessions immediately.

Keep recovery methods current: Make sure your recovery email and phone number are up to date, controlled by the business and difficult for others to guess or access.

Limit financial exposure: Set lower limits or alerts on cards linked to ad accounts so unusual spending is noticed quickly and losses are capped.

Keep devices updated and protected: Install updates for phones, computers and apps, and use reputable antivirus or security tools where appropriate.

Create an incident plan: Know who will act if an account is hacked, including who can contact the platform, pause ads, notify customers and report the incident.

PRO TIP

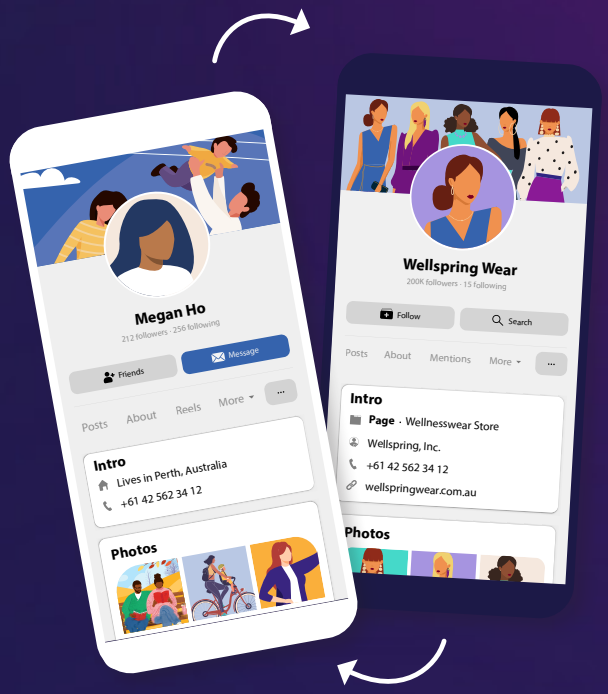
Do a 15-minute social media access audit this week. List every account, who has access, what email is used for recovery, whether MFA is on, and which credit card is linked to ads. Remove anything you no longer need.

Why you need to separate personal and business accounts

Many small business owners create Facebook, Instagram or TikTok business pages using a personal account because it is quick and familiar. In some cases, platforms require a personal profile to create or administer a business presence.

The risk is not the personal profile itself. The risk is relying on one personal login as the main gateway to your business assets, ad accounts and customer channels.

If that personal account is hacked, cyber criminals may also gain access to your business page, ad account, customer messages and payment methods. Recovery can be slow, stressful and sometimes unsuccessful if the business has not set up the right permissions and recovery options.



Set up safer separation

Use business contact details: Use a business email address for business profiles, platform notifications and account recovery wherever possible.

Do not share personal logins: Give staff, agencies and contractors their own access through page roles, Business Manager, Business Center or other official platform tools.

Keep content separate: Use personal accounts for personal content and business accounts for business activity. Avoid posting business-only information through personal profiles.

Add at least two trusted admins: Avoid having a single point of failure. Make sure more than one trusted person can help recover access if an account is compromised.

Review access regularly: Schedule a quarterly check of admins, partners, connected apps, payment methods and recovery details.

CyberWardens.

Platform starting points

Each platform manages business accounts, advertising access and security settings slightly differently. Rather than relying on shared passwords or informal access, set up your social media accounts using the business tools provided by each platform. These tools allow you to assign the right level of access to staff, agencies or contractors, keep ownership with the business, and add extra protections such as two-factor authentication.

Meta

Manage Facebook Pages, Instagram accounts and ad access through Meta Business Suite or Business Manager. Use roles and permissions rather than shared logins, and enable two-factor authentication for anyone with access.

TikTok:

Use TikTok Business Center or TikTok Ads Manager for business and advertising access. Turn on two-step verification, ideally for all members with access to the business account.

LinkedIn:

Use Page admin roles and Campaign Manager permissions so team members can manage company activity without sharing one login.

If something goes wrong

- Change passwords and passphrases immediately, starting with email and admin accounts.
- Log out unknown devices and remove unfamiliar admins, apps or integrations.
- Pause ads and check payment activity.
- Contact the platform's official support or account recovery centre.
- Tell customers what happened if they may have received scam messages or seen harmful content.
- Report cyber crime or cyber security incidents through cyber.gov.au/report.

Real life story

Aami Mills, small business owner

Aami Mills, founder of cloth nappy brand Mimi & Co, was preparing for the biggest moment of her business life: a national TV appearance on Shark Tank in September 2023. The exposure promised to send her business soaring.

But hours after the episode aired, cyber criminals hacked into her Meta accounts, locking her out of Facebook and Instagram and running violent ads using her credit card. Over $10,000 was spent before she could intervene.

"My personal Facebook page was linked to my business page, so they were able to get access to my advertising account," she says. "I would try and reset my password and get a message saying 'we've sent it to this email'. And I'm thinking: 'Oh my goodness, that's not my email, that's their email'."

Her brand, years in the making, was suddenly being used to spread harmful content. She admits the hackers were able to get access as she hadn't implemented multi-factor authentication. Meta's support, she says, was "slow and limited" and her Facebook page was never recovered.

"*It was a very expensive lesson in hindsight*," she says.

Aami has since strengthened her online defences with stronger passphrases, multi-factor authentication, secure recovery methods and by completing the Cyber Wardens course. Now, she shares her story to warn others.

Get started with Cyber Wardens

Cyber Wardens offers free, practical cyber security training for small business owners and employees.

The courses are self-paced, jargon-free and designed for everyday Australians.

Visit **cyberwardens.com.au** to start today