Australian Government

Australian Small Business and Family Enterprise Ombudsman

Using social media securely

Using social media can be a valuable way to grow and increase awareness of your business with existing and potential new customers.

However, it is important to not overlook important security elements – including how to reduce the risk of your social media accounts being hacked. We have helped many small and family businesses across various digital platforms to resolve their disputes, and want to share with you some simple cyber security tips and practices to protect yourself from being hacked:

- Use multi-factor authentication (MFA) or two-factor authentication (2FA) – MFA and 2FA are security features that help protect your Meta account by requiring users to have two forms of identification to access the account. Scan the QR code to learn more about enabling 2FA on your Meta account.
- Choose a strong password and change passwords frequently.
- Update your software and back up your files regularly.

When operating your business online, consider these tips and practices for online safety:

Setting up

- Create your profile with the level of privacy and settings you are comfortable with, now and into the future.
- Make sure you can remove other users or profiles connected to the account and can control their level of page access.
- Confirm you can turn ads on or off and can remove or update advertising payment information.
- Have your account/s set up so that platforms can communicate with you via an app, text message or email to help with account recovery.
- Be aware of and follow the platform's community guidelines. If these guidelines are breached, your business can indefinitely be suspended from the platform.
- Create a separate payment method that is only used for your social media account/s. Set a limit to the amount of spend that your business can manage until a fraudulent transaction can be refunded. This limit will help ensure that, if your payment card or bank account is compromised, only a certain value of fraudulent payments can be made while you are reporting the activity or disabling the card.
- Be prepared: keep your account details in a safe place. If your account is hacked and/or disabled, you may need to provide the URL for all your pages/accounts, the phone number and email address for your account/s and a screenshot of your page/s with the business name.
- Consider expanding your business online presence to more than one platform. If your account is disabled, you can use the other platforms to continue to operate and keep your business going online while you get your compromised account back and running.

Allowing other people to access your account

- Remember – you wouldn't give a person you have just met the keys to your business or your house, so only give access to your business account to trusted individuals. Keep in mind that not all users require full admin access, partial access is often an option.
- As the account creator or main admin, you are responsible for the content posted on the account. This means you need to act quickly if content is posted that does not align with your business' branding, messaging, values, or the platform's community guidelines.
- Ensure any users with access to your business account are cyber security aware by briefing them on these tips.
- Consider the risks of your business account being linked to another user's personal account. Be aware that if a linked personal account is hacked, this may result in your business account being compromised or disabled.

For more information visit www.asbfeo.gov.au/sm-securely

Australian Government

Australian Small Business and Family Enterprise Ombudsman

Using social media securely

If your account is hacked and/or disabled

- If you are hacked, visit the Facebook Help Center (www.facebook.com/hacked) or the Instagram Help Center (www.instagram.com/hacked) to learn how to secure your account. Meta will ask you to change your password and review recent login activity.
- Report your issue immediately with Meta and remember it may take time to resolve it. Keep a copy of the details and number of your report.
- If you have been hacked, only communicate with Meta (or if using a different platform, a verified individual), and not the hacker.
- If you have been hacked or involved in a scam, visit IDCARE for small business (www.idcare.org/smallbusiness) website to lodge your issue with them. This is a free service for small businesses.
- If Meta has been unable to resolve your issue, or if IDCARE is unable to assist, we may be able to help. Fill in our online form (scan the QR code below) where we may be able to contact Meta on your behalf.
- If you have been a victim of a cybercrime, scam or been hacked, you need to report it to the Australian Cyber Security Centre's (ACSC) (www.cyber.gov.au). The ACSC will be able to provide you with further advice on how to respond and protect yourself.

If you're having trouble logging into your Facebook account, review these steps

Learn more about what to do if you think your account is hacked

Learn more about what to do if you can't reset your password because you don't have access to your email address or phone number

Stay alert

- Be aware of new and common scams by checking Scamwatch (www.scamwatch.gov.au).
- Regularly review your business practices to minimise security risks.
- Never click on a link or message, verify where it has come from and where it will take you to (especially if your account has been hacked). Only contact businesses or government using contact information that you find yourself from their official website or app. If you're not sure, delete and report the link or message.
- The Australian Cyber Security Centre (cyber.gov.au) have guides and resources to help small businesses stay secure online.

ASBFEO's online dispute form

Scamwatch

Australian Cyber Security Centre

For more information visit www.asbfeo.gov.au/sm-securely