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 that you don't overlook important security elements when operating on social media, 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 help protect yourself from being hacked (please note that the links below are to Meta platforms, and you may find similar materials on the websites of other platforms that you use):

- 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, and that you can easily control and manage 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 Meta (and other platforms) can communicate with you either via an app, text message or email to help with account recovery (should you need it).
- Be aware of and follow the platform's community guidelines. If these guidelines are breached, your business can be indefinitely suspended from the platform.
- If you are thinking of setting up an account, or already have one, 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
  - 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.

Australian Government

Australian Small Business and Family Enterprise Ombudsman

Using social media securely

- 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.

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 Meta report.
- If you have been hacked, always be sure you are communicating with Meta (or if using a different platform, a verified individual) and not the hacker.
- For more information on Meta accounts, scan the QR codes below:

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

- If you have not been able to resolve your account issue with Meta through their support channels, use ASBFEO's online form (scan the QR code below) to lodge a dispute for assistance.

Stay alert

- Be aware of new and common scams by checking Scamwatch (www.scamwatch.gov.au) which helps you spot, avoid, and report scams.
- Regularly review your business practices to minimise security risks.
- Before clicking on a link or message your account has received, verify where it has come from and where it will take you to (especially if your account has been hacked). You can generally verify unknown links by 'hovering' over the URL to see the exact website to which the link is directed (noting that a URL shown may disguise the actual link that is disclosed when hovering).
- 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