

FACT SHEET

Social media security for small businesses

Common risks associated with social media

Social media is often seen as an attractive target for scammers. Social media account details may be phished, leading to impersonation and other misuse. Business impersonation can lead to businesses suffering reputational damage leading to a loss of customers. Customers of the business may also suffer financial loss or compromise of their personal information if they engage a scammer through a compromised business social media account.

To mitigate these risks, small businesses should implement strong security measures, including enabling multi-factor authentication (MFA), regularly reviewing privacy settings, and educating employees about cybersecurity practices.

Detecting business account problems

Common signs there may be a problem with your social media account:

- You see another profile/account using the same name (personal or business) and some of your photos, logos or posts.
- You don't have a social media account, but you learn about one that uses your photos, personal information or business details.
- Friends or customers tell you they have been receiving friend requests from a social media account with the same name.
- You do a reverse image search of one of your own photos and see it appears in a different social media account. When you go to that account, you see that it is claiming to be you or your business.

Preventing social media business account problems

- **Choose a secure password** you do not use for other online accounts. Consider using a password manager to ensure it is unique and not able to be guessed.
- **Use a business email address** for your business social media accounts.
- **Ensure you are using the correct website before logging in.**
- **Ensure all business members use 2FA** to login, using a third-party authentication app.

FACT SHEET

Social media security for small businesses

- **Have more than one admin user**, so that if one is away or leaves your business, you still have access to the account.
- **Manage shared accounts** – limit account access and keep records of login details, role-based access permissions and any linked personal accounts
- **Be aware of who in your business has login details** for your account, and remember to update passwords regularly, particularly when employees who have access leave.
- **Create a social media policy** for your business accounts and users that outlines acceptable information sharing, account management, phishing recognition, and procedures for reporting and recovering hacked accounts.
- **Keep backups of information** and data such as posts and customer contacts if they are important to you or your business.
- **Monitor social media account activity** and security alerts. Monitor use of your brand and business name and report suspected fraud, impersonation or scam posts and profiles.
- **Regularly review your social media privacy and permission** settings. Be cautious when sharing business locations and information.
- **Check out the advice** from [Facebook](#) and [Instagram](#) on business account security and reporting procedures.

FACT SHEET

Social media security for small businesses

Responding to business account problems

- **Contact the account hosting platform** immediately if someone has gained access to your account, created an account impersonating your business or your brand is being used in scam ads
 - Check out the advice from [Facebook](#), [LinkedIn](#), [Instagram](#) and [X \(Twitter\)](#) on compromised accounts.
 - Report account impersonations to the appropriate platform: [Facebook](#), [Instagram](#), [LinkedIn](#), [X \(Twitter\)](#)
- **If you have stored your credit card details** on the social media account or linked accounts, contact the issuer immediately to cancel the card.
- **Notify the relevant document issuing organisations** for any of the credentials that may have been stored in your account.
- **Let your employees and customers know** that your account has been accessed or impersonated, using a method other than the social media platform or its linked accounts.
- **If you believe that the password for your account has been compromised**, ensure that the password is not used for other online accounts to prevent further misuse. Also consider enabling MFA for all accounts, where it is available.

FACT SHEET

Social media security for small businesses

Protect your customers from scams

Help protect your customers from losing money or personal information to business impersonation scams:

- **Educate on communication methods:** Inform your customers about how your business communicates with them. This may help your customers identify genuine messages and spot potential scams.
- **Check hyperlinks:** Remind customers to verify the legitimacy of any messages before clicking links. Let customers know whether you will send links and provide them with a clear way of determining the legitimacy of any messages.
- **Establish a reporting process:** Create a straightforward process for customers to report impersonation websites to you. This makes it easier for you to act quickly.
- **Communicate impersonation alerts:** If your business is targeted by impersonators, promptly alert customers through warning on social media, your website, and at points of sale. Include links to Scamwatch for [reporting](#) and [advice](#).



For additional support or information, contact IDCARE by submitting a [Get Help Form](#) or call 1800 595 170

Sharing & Disclaimer

IDCARE is Australia and New Zealand's national identity and cyber community support service. IDCARE is a not-for-profit and registered Australian charity. © 2024 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the assessment or any accompanying data provided.