FACT SHEET

FACT SHEET: Facebook

Facebook is a free social networking website supporting over 1 billion individual users, groups and businesses worldwide. Users can send and receive written messages, share photos or videos and links to news or other content, stream videos and play games. Facebook also supports interactive, real time online chat and is financially supported through advertising. Given Facebook's reach, messaging and advertising features, criminals can exploit these, making users susceptible to scams, identity theft and cybercrimes. By reviewing your Facebook security settings and being conscious of how you use Facebook you can mitigate these risks.

Preventing Facebook account problems for personal accounts

- Check out the advice from Facebook on personal account security.
- Ensure you are using the correct website before logging in.
- Choose a secure password you do not use for other online accounts.
- Use two factor authentication (2FA) to login, and choose a third-party authentication app.
- Log out of Facebook from shared computers.
- Be careful when choosing whether to accept a Facebook friend.
- Keep your information/profile private. If you don't want people to know – don't share.
- Avoid clicking bait links that appear in your feed and in messages.
- If you are prompted to login to your account by clicking on articles, do not; they may use software that captures your information.
- Set up trusted contacts who can send you recovery codes and URL links if you ever get locked out of your account. Make sure these are people you know well, such as family members or long-time friends who you meet regularly in person, not someone you know only online.
- Finding the security settings:
  1. Select **Account** at the top right hand corner of your logged in Facebook profile
  2. Select **Settings**
  3. Click **Passwords and Security**

Preventing Facebook account problems for business accounts

- Check out the advice from Facebook on business account security.
- Ensure you are using the correct website before logging in.
- Choose a secure password you do not use for other online accounts. Consider using a password generator to ensure it is unique and not able to be guessed.
- Ensure all business members use two factor authentication (2FA) to login, and choose a third-party authentication app.
- Regularly review your Page roles and permissions.
- Be aware of who in your business has login details for your account, and remember to update passwords regularly, particularly when staff members leave.
- Have more than one admin user, so that if one is away or leaves your business, you still have access to the account.

FACT SHEET

Detecting problems with your Facebook account

There are two main problems reported to IDCARE about Facebook accounts.

- Someone has accessed or taken over my account, often meaning that:
  - ☐ You can no longer login to your account as your email address and/or password have been changed.
  - ☐ Your personal information has changed, such as your birthday or the name of your account.
  - ☐ Posts appear that you did not write.
  - ☐ Messages have been sent from your account that you did not write.
  - ☐ You have new friends that you did not accept.
  - ☐ Friend requests have been sent from your account to unknown people.
  - ☐ Your friends, family or other businesses report receiving strange messages from your account.
  - ☐ You receive an alert that your Facebook account has been logged into from a device or location unknown to you.
  - ☐ Changes are made to your linked accounts, such as Facebook Marketplace, Messenger or Instagram.
  - ☐ You see new accounts linked to your Facebook account.
  - ☐ You see a new Facebook account linked to your Instagram or Facebook Marketplace accounts.

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

Responding to Facebook account problems

- ☐ Contact Facebook immediately if someone has gained access to your account, is impersonating your Facebook account, or has created a Facebook account impersonating you or your business but you don't use a Facebook account.
- ☐ Check out Facebook's Fact Sheet which we have posted on the IDCARE website.
- ☐ If you have stored your credit card details on Facebook 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 friends, family and customers know that your account has been accessed or impersonated, using a method other than Facebook or its linked accounts.

For additional support or information, contact IDCARE by submitting a Get Help Form or call 1800 595 160 (Aus) or 0800 121 068 (NZ).

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. © 2021 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.