



## **Facebook Security**

## **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, link posts to news or other content, stream videos and play games. By reviewing your Facebook security settings and being conscious of how you use Facebook you can mitigate risks to your account and personal information.

### **Quick Facts**

- in Facebook has the benefit of being more open and social than traditional communication tools, but usage does not come without its risks.
- Facebook give users the option to enable email or login notifications that alert users whenever their account is logged into.
- Facebook also allows users to check their security settings to ensure they are the only person logged into the account.
- Facebook has quickly become a place for businesses to advertise and sell products and services.

#### **Prevention**

- **i** Ensure you are using the correct website before logging in.
- Choose a secure password you do not use for other online accounts.
- 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; this is software that captures your information.
- To review your settings:
  - 1. Select Account at the top right-hand corner of your logged in Facebook profile
  - 2. Select Settings
  - 3. Review options under Security











# **Facebook Security**

#### **Detection & Response**

- If you receive an unusual message from friends or family, do not respond or click on links provided; rather confirm its validity by reaching out to them via other communication methods.
- Request that friends and family do the same if they are feeling unsure about a message or request.
- inform Facebook immediately if you suspect fraud. Facebook has the option to 'report' a profile that is impersonating someone you know, representing a business or organisation, is annoying you, or sharing inappropriate or offensive material.
- Report if your own account has been compromised and follow Facebook's official account recovery instructions
- If someone you know is threatening or bullying you, screen shot the evidence to provide to police if necessary.



### **More Social Media Security Facts**

IDCARE have a number of Social Media Security Fact Sheets to help you detect, prevent and respond to problems you may have. Please see the below Fact sheets on:

- Twitter Security
- LinkedIn Security
- Instagram Security

## Other Fact Sheets

Credit Reporting Agencies

**©** Engaging Organisations

Devices and Technology

Scam Prevention and Education

Social Media

**D** Your Rights

Disclaimer © 2018 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.



( AU: 1300 432 273 or NZ: 0800 201 415



