

In your reflective activity, you should have covered the points below.

- You chose a very weak password for your SocialBook account.
- You did the right thing by immediately alerting stakeholders that your SocialBook account has been hacked. They rely on it for information about your service and are now at risk because they will trust whatever is posted on it. Your swift response will limit the number of people effected.
- The SSSC Code of Practice for Social Service Workers says you must not put other people at unnecessary risk. By promptly informing stakeholders about the SocialBook account being breached, you reduced the risk and demonstrated you were meeting the standards expected of a social service manager.
- However, your choice of password allowed someone to easily hack the account and there will be people adversely affected because of this.
- You need to do more learning to develop a better understanding of how previous training can be forgotten or become outdated. The online safety and security training opportunity offered an opportunity to refresh existing knowledge and introduce important information about new online threats and how to protect against them.
- You need to make sure your team attend online safety and security training regularly. The advice provided by such training evolves and adapts to the threats we face and what was best practice several years ago can be dangerous today.
- When online safety and security training was offered, the right thing to do was accept the invitation.