



In the fifth issue of the ThinkUKnow e-newsletter, we provide advice on how to remove offensive social networking profiles and how to protect your accounts and devices.

Removing Offensive Profiles

People may create fake profiles or deface existing profiles on social networking services as a form of cyber-bullying or electronic aggression. This can be quite distressing for young people and adults as well. If this happens to you or your child, there are a number of different actions you can take. Remember, you may want to keep a copy of the offensive profile as a record of the cyber-bullying incident.

1. If it is your existing profile that has been defaced you can:

Delete the profile

On MySpace Australia: Select "Account Settings" from your personal home page and click on the "Cancel Account" option. On the new page, select the "Cancel My Account" button. This will send an email to the email account you used to set up your MySpace account. Follow the instructions in this email to remove your account. [Visit MySpace for more information.](#)

On Facebook: Select "Settings" and then "Account Settings" once you are signed in. Select "Deactivate Account" and follow the instructions.

On Bebo: Once you have signed in to your account, select the "Settings" option. On the new page, click on the "Cancel your Membership" link and click on the YES button. [Visit Bebo for more information.](#)

Unfortunately, your account may not be deleted immediately and you need to be aware of this. It may take some time for changes to take effect.

Undo all the changes made.

If you are not willing to delete your account the first thing you need to do is change your password. This can be done through your account

Time2Talk

This section provides some useful conversation starters for talking with young people about their use of technology.

Have you ever seen a profile that has been defaced or a fake profile?

Do you know what a strong password is?

Have you ever shared your password with a friend?

What would you do if you came across someone's phone or device that was unattended?

Protecting Your Accounts and Devices

There are a number of steps you, and your child, can take to protect devices and online accounts from being used as part of cyber-bullying.

- Use a strong password and keep it secret. A strong password is one which contains a mixture of upper and lower case letters, numbers and keyboard symbols. You should not share your password with anyone; however, it may be useful to have your child share their passwords with you in case they forget them.
- Always log-out of your account when you are finished. This will ensure that people cannot access your social networking, instant messaging or email account when using the computer after you. This is particularly important if you are using a public, school, or shared computer. You should never use public computers when sharing sensitive personal information such as when banking online.

settings. It is important that this is your first step so that the person who defaced your profile can no longer sign in to your account. Now you can remodel your profile to remove any nasty comments, images or other posts.

This is also a good opportunity to block people from being able to access your social networking profile. You may wish to change your privacy settings to a higher level at this time also.

2. If someone has created a fake profile in your likeness, you can contact the administrators of the social networking service to have it taken down.

On MySpace Australia:

- When you are viewing the fake profile, select the "Report Abuse" option at the bottom of the page and then choose "Imposter Profile" as the basis of your complaint. Follow the instructions on how to have the profile taken down.
- If you are a teacher or employee at an educational facility and discover a fake profile in your likeness, contact schoolcare@myspace.com from a school email address and provide the URL of the profile, your name and title, the contact details of the school at which you are employed and a description of why the profile is fake or offensive.

On Facebook:

Alert Facebook administration by using their "Contact Us" facility.

On Bebo:

Alert Bebo administration by using their "Contact Us" facility.

- Password protect your devices if possible. Some laptops, mobile phones and portable gaming devices offer the option of locking the device so that a password or PIN is required to access and operate the device. You should investigate whether this option is available on your and your child's devices.
- Keep your devices with you where possible. This will limit the opportunities for people to access your devices and use them without your permission. When you are not able to have your devices with you, they should be stored in a secure location.

Update on ThinkUKnow Australia

As of Term 1, 2010, ThinkUKnow Australia will be rolled out nationally. This means that schools outside of the pilot states (Australian Capital Territory, New South Wales, and Victoria) will now be able to book a ThinkUKnow presentation.

We cannot guarantee that we'll be able to provide presentations for non-metropolitan areas but we are developing solutions for regional areas.

Expressions of interest for booking school presentations can be made by [contacting ThinkUKnow](#).