

**Social networking sites, like Facebook, are great tools that give teens an opportunity to express themselves and communicate with their friends.**



For the most part, teens use social networking for self-expression. They chat, share and interact with real world friends - socialising almost exclusively with people they know. While it's only natural for parents to be concerned about cyber stranger danger, stats show that a young person is more likely to fall victim to harm from their peers, or suffer the consequences of their own online actions.

While our online safety pointers don't focus on the old 'stranger danger' warning, they do concentrate on the more realistic concerns around posting content that could come back to bite them with school authorities and future employers. So, go ahead - run through the following tips and pick up some safe social networking practices when using Facebook, for you and your family.

## Delete delete delete!

Sometimes in the heat of a moment or simply without thinking, it's easy to post something you wish you hadn't. It's easy to unintentionally reveal personal info (like where you live) or even feel pressured into sharing a risqué photo. Remember:

- Stick with your gut feeling and if you're unsure, just say 'No'.
- Scan through your profile and remove any personally identifiable info like your address or phone number.
- Delete any unwanted wall posts from friends that might be inappropriate.

## Tweak their settings

It's important to keep your online content private and away from prying eyes.

- Visit Account **Privacy Settings** ➔ **Sharing** on Facebook and set this to **Friends only**.
- Check the security of photo albums, remembering that each one has its own privacy setting.
- Teens should register as under aged users. 13 to 18 year olds can take advantage of extra privacy settings (like restrictions where only friends can see if they've 'checked in' somewhere).

## Stop, Block and Tell!

While you can't un-see something you wish you hadn't, you can do something to stop it by reporting to Facebook and talking to someone you trust.

- Use **Report this photo** for inappropriate images, or **Report/block this person** if you stumble across a fake or offensive profile.
- Don't respond to threatening messages - they don't deserve your attention.
- **Stop** any contact with someone being aggressive. **Block** any future contact attempts, and **tell** a trusted adult.

## Preview profile

Take a look from the other side! Use Facebook's privacy settings tool to find out what info from your profile is on show for the rest of the world to see.

- Visit **Account Privacy settings** ➔ **View settings** ➔ **Preview my profile**.
- Delete anyone who's not a real life friend (they could be a creep or someone dodgy).
- Conduct regular 'spring cleans' and remove anyone you don't interact with from your friends list.

## Safety starts at home

Cyber safety can be as simple as a good anti-virus program, sensible privacy settings and setting simple ground rules.

- Beef up your internet security- update your antivirus, turn on your firewall, run automatic updates, pin lock mobile phones and change passwords regularly.
- Encourage your family to talk and share. If they run into any issues, they should be able to talk openly without fear of losing their internet privileges.
- "Friend" your own kids - but spare them the mortal embarrassment of commenting on their photos or posting on their wall ;)
- Keep mobile phones switched off, and on the kitchen bench at bed time.

