Facebook safety tips for parents

Are you aware of the recent statistics that have emerged from places like the Cyberbullying Research Center?

- At least **one in five** kids are targets of cyberbullying, which often leaves deep emotional scars.
- **One in five** teens say they've received unwanted sexual solicitations online.
- **One in five** Facebook users are exposed to malware links in their newsfeed–putting kids in danger of being victims of viruses or account hacking.

Facebook has millions of users and grows every day, connecting all kinds of people all over the world. Unfortunately, some of those people pose a risk to your family.

At the same time, Facebook has become an important social center for kids. It's a great way for them to stay connected and enhance friendships.

That's why we're sharing a number of tips and an excellent tool to help your family outsmart the risks on Facebook.

Share these tips with your family

- **Protect your privacy with these tips.**
- **Make sure your Facebook password is strong with these tips.**
- **Think twice before accepting friend requests** — make sure you know that person and are willing to share your personal data with him/her.
- **Do not enter your address, phone number, or other ways to contact you** in your Facebook profile.
- **Be choosy about Facebook application permissions** — don't give applications the possibility to access the information of your private friends and even talk to your friends in your name. You can review the apps you have authorized by going to your Facebook "Application Settings."
- **If you don't know the sender** — don't open it! Booby-trapped attachments are often disguised in clever thank you notes or e-greetings.
- **Be suspicious of Facebook messages** that request personal information.
- **Be careful with messages that look like they are from popular sites.** While they may link to a third-party site that makes them look official, they are often created by thieves or scammers.
- **Watch for red-flag phrases,** like "You have won!" or "Verify your account." Genuine firms don't send messages like that.
- **Use a good Facebook security program** like **ZoneAlarm® SocialGuard**

Use your Facebook privacy settings

It's important to understand what information Facebook considers public. Your default privacy settings might be revealing much more than you intended.

- **Start by taking the formal Facebook tour at:http://www.facebook.com/privacy/explanation.php**
- **Anyone may be able to send you messages on Facebook. We suggest limiting messages to friends only. See this Facebook page to learn how to limit who can message you.**
- **Continue by customizing your privacy settings in your Facebook Account > Privacy settings**

There are many settings and services related to your privacy and multiple places to edit the same settings. So it can all be somewhat confusing. Safeguarding your privacy is an ongoing process that requires your ongoing attention because Facebook continually redesigns its interface and settings.

It's worth taking a look to ensure that you're getting exactly what you want out of Facebook!

Make sure your Facebook password is strong enough

One of the most common risks is having your Facebook account hacked. Many people create passwords with real-life meaning, which makes them easy to memorize and reduces typing errors. For example, private names, birth dates, counties, and hometowns are popular password sources but they make weak passwords.

Another common mistake is to use the same password on few different services. For example, your email account, Facebook account, and computer. This makes a hacker's life easier.

So what is a strong password?

- A strong password is difficult for humans and computer programs to guess.
- A strong password consists of at least six characters, including a combination of upper and lower case letters, plus numbers and symbols.

Source: Check Point Software
Date Published: April 2011
Link: http://www.zonealarm.com/security/en-us/zonealarm-socialguard-facebook-parental-control.htm