

# **Security on Social Networking Sites**

## **Module 11**

Simplifying Security.



**Certified Secure Computer User**

**Module 11: Security on Social Networking Sites**

**Exam 112-12**



## Module Objective

In recent years, social networking sites have witnessed a meteoric rise in the number of registrations per day. In fact, this trend is forecast to increase in the coming years. People tend to accept these sites as a better means to build and nurture their social networks. As a result, a lot of **personal information** gets posted on the social networking sites. The information posted by the users, however, may be used by **scammers** to **steal identity**, among other offenses. This module talks about security on social networking websites.

This module will familiarize you with:

- |  |  |
|--|--|
| • Social Networking Sites                            | • Facebook: Security Tips                              |
| • What Is a Profile?                                 | • Staying Safe on MySpace                              |
| • Top Social Networking Sites                        | • Security Measures                                    |
| • Security Risks Involved in Social Networking Sites | • Social Networking Guidelines for Parents and Teacher |
| • Staying Safe on Facebook                           |  |



## Module Flow

Introduction to Social Networking Sites

---

Social Networking Security Threats

---

Staying Safe on Facebook

---

Staying Safe on MySpace

---

Social Networking Guidelines for Parents and Teacher

---



## Social Networking Sites

Social networking has been around for a long time. Social networking refers to the gathering of people with similar interests/hobbies. Recreational clubs and societies are examples of social networking groups. **Social networking websites** have evolved from face-to-face networks. Online social networking takes place over the Internet.

Social networking sites allow users to build **online profiles**, **share information**, pictures, blog entries, music clips, etc. They allow users to connect with their friends, friends of friends, and friends who have not been in contact for a while as well as to be friends with people who share the same interests. These sites allow users to create a list of other users with whom they can share information.

Social networking sites allow users to **manage** their **contacts** and find new ones. Networking sites such as LinkedIn target professionals, whereas Facebook, MySpace, Bebo, etc. are general interest community sites and allow for smaller communities with common interests to form.

Using social networking sites, users can find a job, meet people, read movie reviews, and find out if the new restaurant is worth their money. At the same time, social networking sites have become the center stage for **identity theft**, **sexual predators** luring children, and numerous **privacy concerns**.

While optimists say that social networking sites help forge new relationships and strengthen old relationships, pessimists believe that social networking sites only isolate users from the real world.

Popular social networking sites include Facebook, MySpace, Twitter, LinkedIn, Bebo, Orkut, Ning, Friendster, and Yahoo! 360.

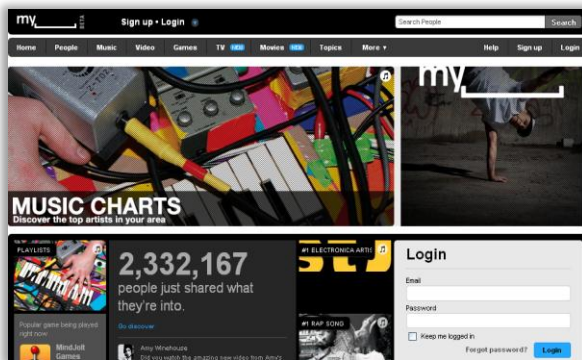


Figure 11- 01: MySpace

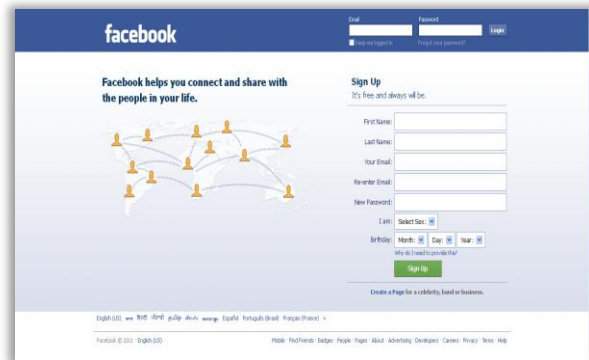


Figure 11- 02: Facebook



## What is a Profile?

A profile is a **collection of information** that defines or describes the user and his or her interests. The main profile page of a person on any social networking site introduces and describes him or her. The information on the profile page allows others to know about the user. This information is also helpful in recognizing friends/acquaintances.

Information the user may post on his/her profile include:

- Names/nicknames
- A personal photo
- Email addresses
- Address
- Phone numbers
- Photos and videos
- Personal interests
- Names of schools, sports teams, and friends
- Groups
- Networks/communities
- Profile updates of friends
- Status messages
- Comments

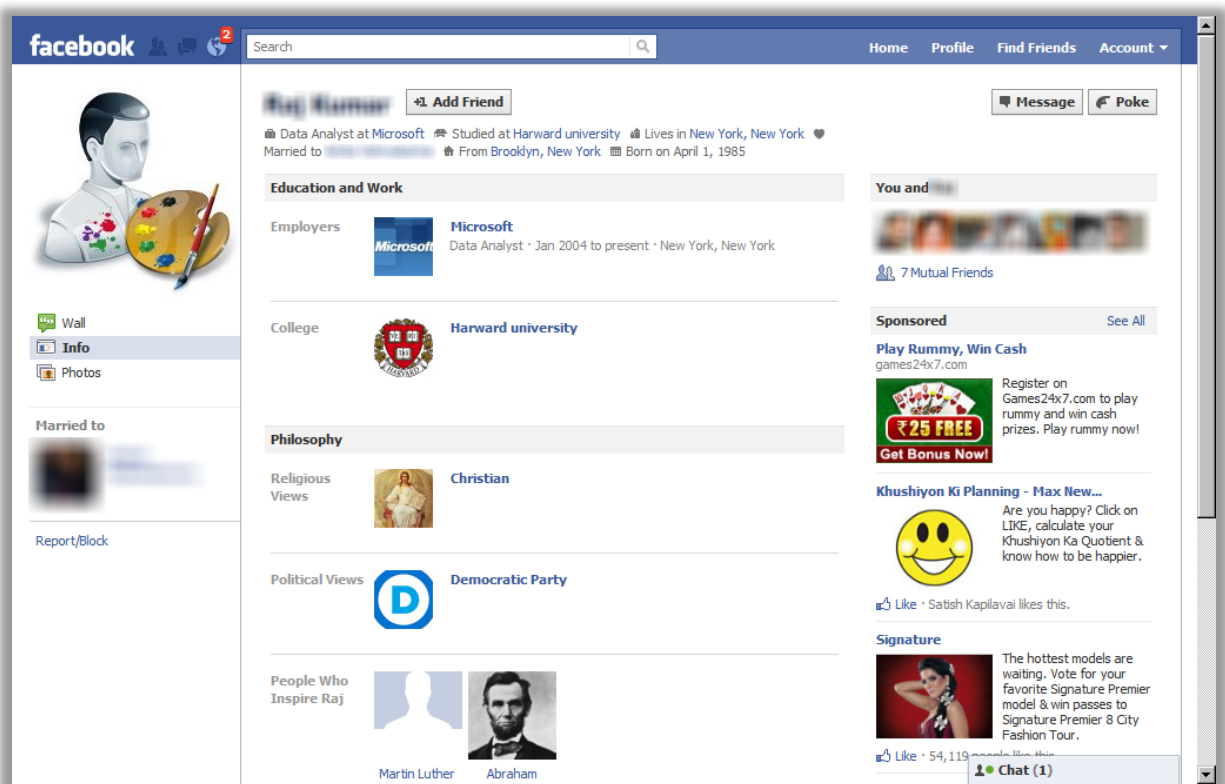


Figure 11- 03: Profile Information



## Top Social Networking Sites

Source: <http://www.ebizmba.com>



<http://www.facebook.com>



<http://www.tagged.com>



<http://www.bebo.com>



<http://twitter.com>



<http://www.classmates.com>



<http://www.mylife.com>



<http://www.myspace.com>



<http://hi5.com>



<http://www.friendster.com>



<http://www.linkedin.com>



<http://www.myearbook.com>



<http://www.myheritage.com>



<http://www.ning.com>



<http://www.meetup.com>



<http://multiply.com>



## Security Risks Involved in Social Networking Sites

Social networking sites have outgrown the basic functionality of networking with friends and relatives. These websites are now used by businesses to **commercialize a product**, draw users to a particular brand, and allow individuals to see their products. At the same time, social networking sites are becoming a **hub for online crimes**. Social networking sites are being used increasingly for identity theft, for cyber-criminals to attract innocent teens into sexual traps, and so on.

Some of the **threats** that users face on social networking sites include:

- Cyberbullying
- Identity Theft
- Phishing Scams
- Malware Attacks
- Site Flaws
- Objectionable Content
- Contact Inappropriate Adults and Businesses
- Overexposure
- Contact with Predators



## Cyber bullying

Cyber bullying refers to the abuse of technology to harass or **threaten Internet users**. Often, it includes **spreading spiteful rumors**, threatening over the Internet, harassment, and stalking. Internet, the new arsenal in bullies' arsenals, outdoes all other previous means of threat such as snail mail and telephone. Also, Internet tools, such as email, instant messaging, digital pictures, and videos, provide a safe haven for cyber bullying. Users communicate a great deal of personal information through these tools, and cyber bullies can access this information to the detriment of the users. Victims can incur **irreparable damage** by the time a cyber-bully is caught, which is not easy to do.

Although cyber bullying is aimed at all Internet users, the young are more likely to be its victims. In fact, with the increasing affinity among children for online social networking, the problem is likely to persist. According to a research by the Pew Internet Project, **39 percent of social network users** had been cyber bullied in some way compared with 22 percent of online teens who did not use social networks.

To avoid cyber bullying, users should:

- **Be careful** about what is posted on the Internet
- Not escalate the situation by responding to the cyber bully with hostility and provocation—bullies may turn even more violent after sensing the victim's hostile reactions. Try to **ignore the bully**. If victims are receiving warning emails, they should change their email address and be cautious when sharing their email ID
- **Document all conversations**, emails, and any other electronic communications
- **Contact the local authorities** if the situation gets out of control or if they are being threatened/ harassed

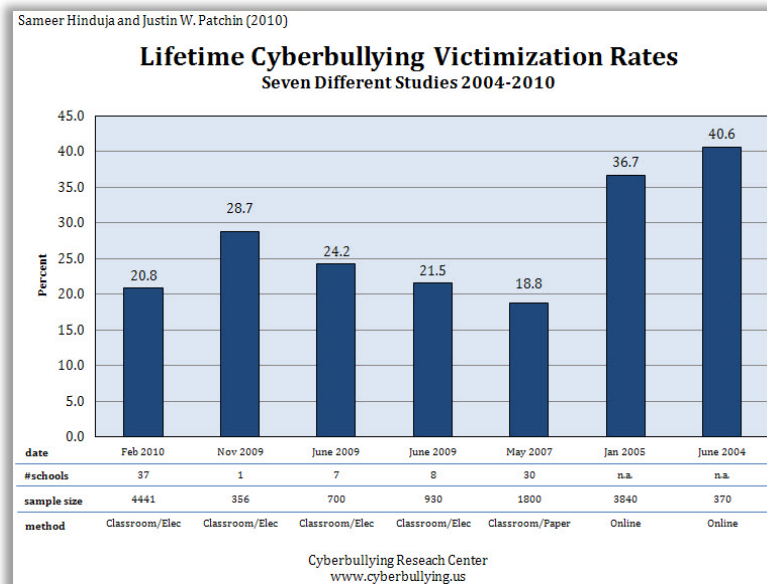


Figure 11- 04: Cyber Bullying



## Identity Theft

With the ever increasing popularity of social networking sites, such as Facebook and MySpace, and the enormous amount of **personal information** being posted, social networking sites are **breeding grounds** for identity thieves.

Users of these sites get carried away when posting their personal information on the sites and provide such personal information like their full name, surname, date of birth, address, contact numbers, email address, etc. Identity thieves can piece this information together to **steal the user's identity**. For example, they may use this information to trace answers to the security questions of the user's online services.

The photos or videos that users upload onto social networking sites can be **misused** by cyber-criminals. They may even **blackmail** the user into revealing more information, ask for a **ransom in return**, or threaten to post them all over the Internet.

The user may be dissatisfied with the online services of his or her bank and may post something on these sites that reveals the name of the bank he or she uses. Paired with other personal information, the identity thief may be in for some **financial gain**.

The identity thieves may also become friends with the users and manipulate them into clicking malicious links or downloading malicious software onto their computer. Then, they can easily steal their personal information. Alternately, an attacker may find the user's name and browse through his/her social profile. He can then write an email based on the user's interests bearing a malicious link or document.

Therefore, to avoid becoming a victim of identity theft, users should:

- Ensure that their **passwords** cannot be easily cracked
- **Be cautious** when clicking links in messages and when downloading applications
- Set their profile to **private** and limit access to only people they trust
- **Not post sensitive information** on their profiles that can be used for identity theft



Figure 11- 05: Phishing Email



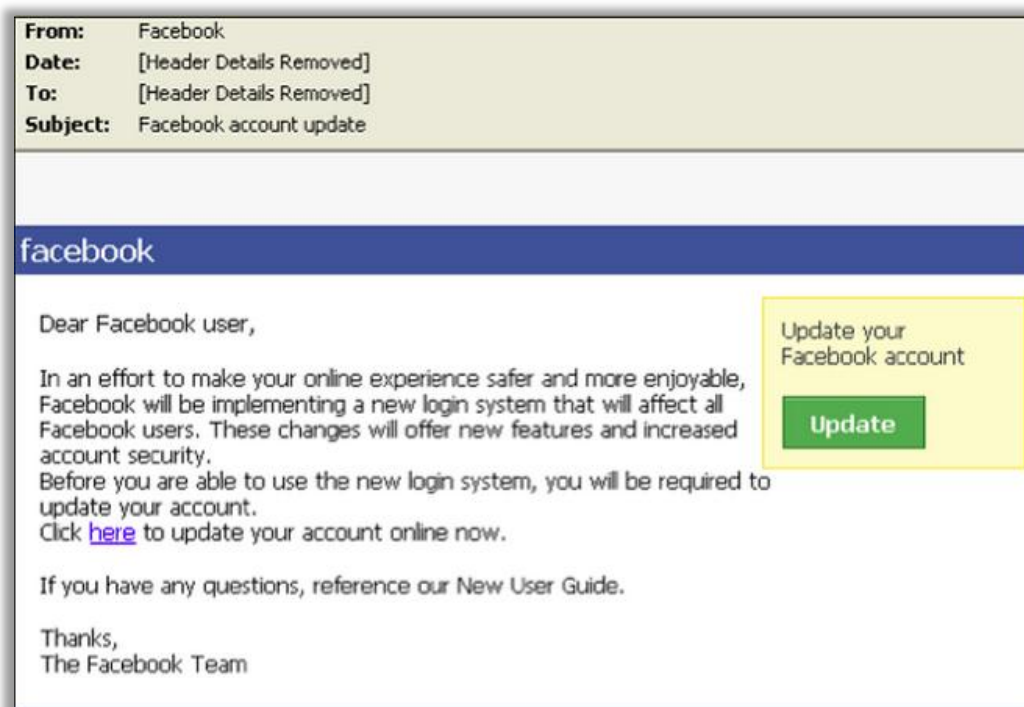
## Phishing Scams

If users are posting their personal information including **email addresses** on social networking sites, chances are high that they may be a victim of a phishing attack. The attacker may send them a **malicious link** to a **phishing site**.

Social networking sites also contain archived messages, user interests, hobbies, etc. The attacker may use this information to send users an **enticing email** that will convince them that it is authentic. Once they click the link, they are **redirected to a phishing** website that looks familiar to the social networking site.

The user then fills in the login details (username and password) just as he or she would do on the social networking site. Now, the user has divulged his/her login information to the attacker. The attacker may then login to their profile and steal all of the information or send phishing links to all of their contacts and steal their information.

Users have to be careful when clicking email attachments. They even have to be weary of email attachments that include a “**password reset**” request. Users should realize that legitimate websites never send an email asking them to reset their passwords.



**Figure 11- 06: Example of Phishing Scam**

If a user clicks the **Update** button shown in the previous figure, he/she is redirected to a site that looks similar to Facebook. Users are then asked to enter a password to complete the update procedure.





## Malware Attacks

Users are led to clicking malicious links via social engineering. Malicious links are sent in the form of messages. Once the user clicks these links, they are **redirected to malicious websites** from which **malware is downloaded** onto the computer. The attacker may then use the user's computer to launch attacks on other computers. The user's computer becomes a **zombie computer** so that the real attacker cannot be traced. The attacker similarly may force other users to click the malicious links and take control of their computers.

The attackers use these zombie computers to attack a targeted website and make the traffic to the website so high that the other users are denied a request to view the website. Facebook, Twitter, and LiveJournal have been victims of such attacks through a malware known as "Koobface."

### To avoid this:

- Do not click suspicious links
- Do not post anything personal on a social networking site and make your profile private by using the privacy settings
- Update your computer with the latest anti-virus and other software

Another method of attack involves applications advertised on social networking sites, which appear genuine; however, some of these applications install malicious code or rogue anti-virus software.

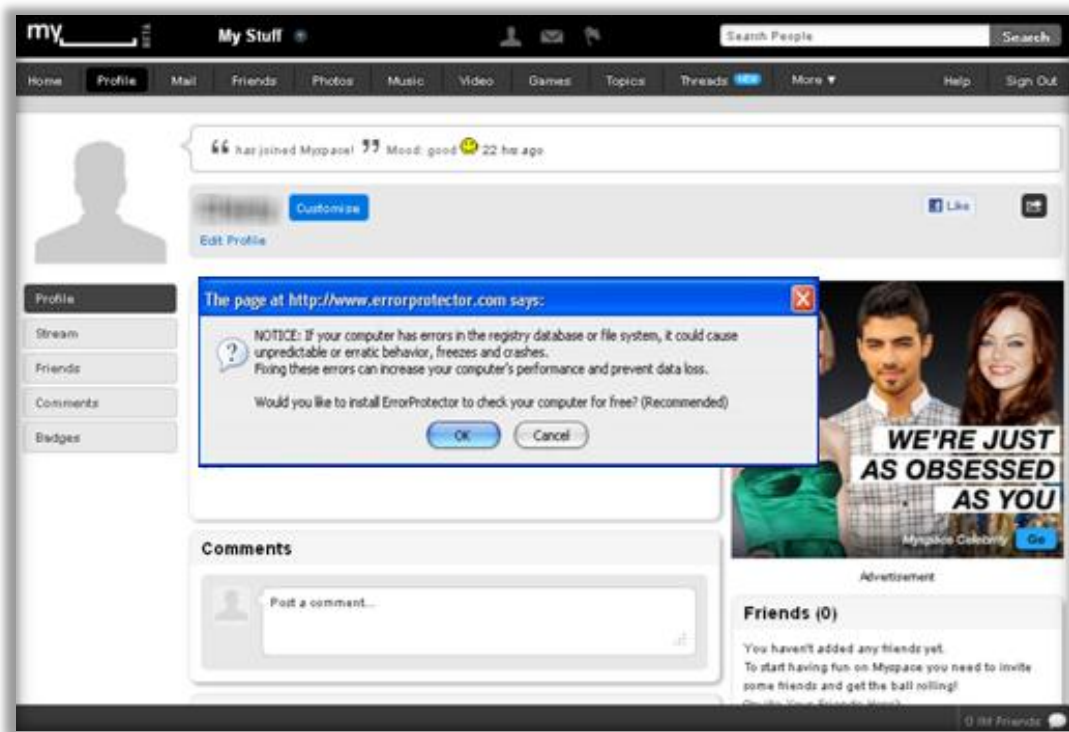


Figure 11- 07: Example of Malware Attacks



## Site Flaws

Like other software applications, social networking sites can also have flaws such as:

- Server-side flaws
- Cross-site scripting
- Cross-site request forgery

These flaws can be used by the attackers to **launch attacks** and steal user information. There have even been instances in which the personal information of the user, such as his or her mother's maiden name, was visible even when the privacy settings of the profiles were on. Often, such key personal information is used as a security question and real-life security check.



## Social Networking Threats to Minors

A study suggests that Gen Y and Z stem the growth of the social networking sites. Children are the major reason for the monumental growth of social networking sites. This makes social networking sites a place for **Internet criminals, pedophiles**, and other threats.

The threats to minors on social networking sites include:

### Objectionable Content:

Although social networking sites do not allow posting objectionable content such as obscene messages, explicit pictures, violent or hate messages, and sexually explicit content such as pornography, some users post them anyway. This content is there for the kids to see until the material is deleted.

### Contact Inappropriate Adults and Businesses:

Various segments of the sex industry (legal and otherwise) have a presence on social networking sites, often to recruit customers and workers. Minors may come in **direct contact** with such sex professionals and organizations. In some cases, teens could become victims of sex trafficking or be persuaded to provide sexually explicit pictures or video for pay.

### Overexposure:

Many community pages may contain material that is not appropriate for children. A child may be involved in posting sexually provocative or incriminating pictures of him- or herself or of friends, publishing personal information that sexual predators could use to learn more about a child or their friends, bragging about exploits, or making threatening and harassing remarks that could have negative consequences.

### Contact with Predators:

Sexual predators or pedophiles on social networking sites may pose as people much younger than their actual age. They may contact children and try to make sexual advances. To avoid this threat, **profiles should be made private**, and parents should ensure that their children do not

post any personal information on social networking sites and should regularly monitor who they are contacting.

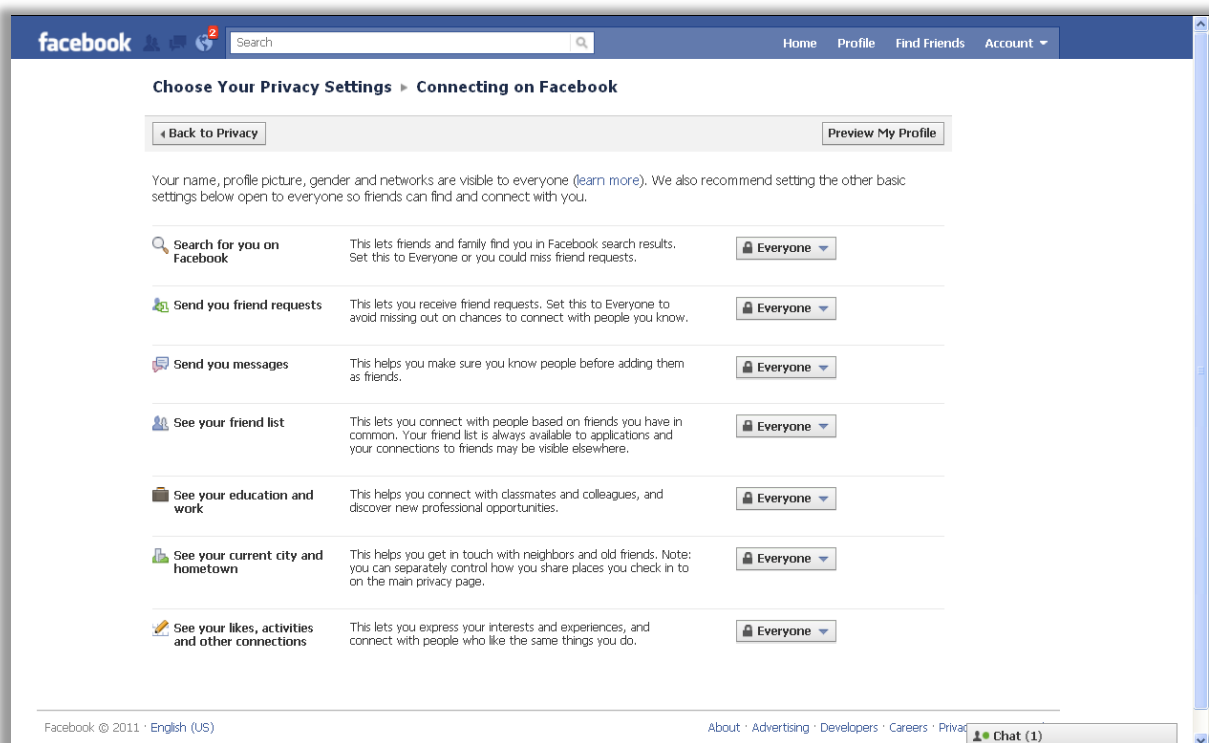
To avoid this issue, most social networking websites have privacy policies for user profiles. The profiles of users less than 18 years of age are automatically set to private on MySpace. Facebook also offers a wide range of privacy setting.



## Facebook Privacy Settings

Facebook allows its users to set the privacy settings for:

- Search
- Friend requests
- Messages
- Friend list
- Education and work
- Current city and hometown
- Likes, activities, and other connections



**Figure 11- 08: Privacy Settings in Facebook**

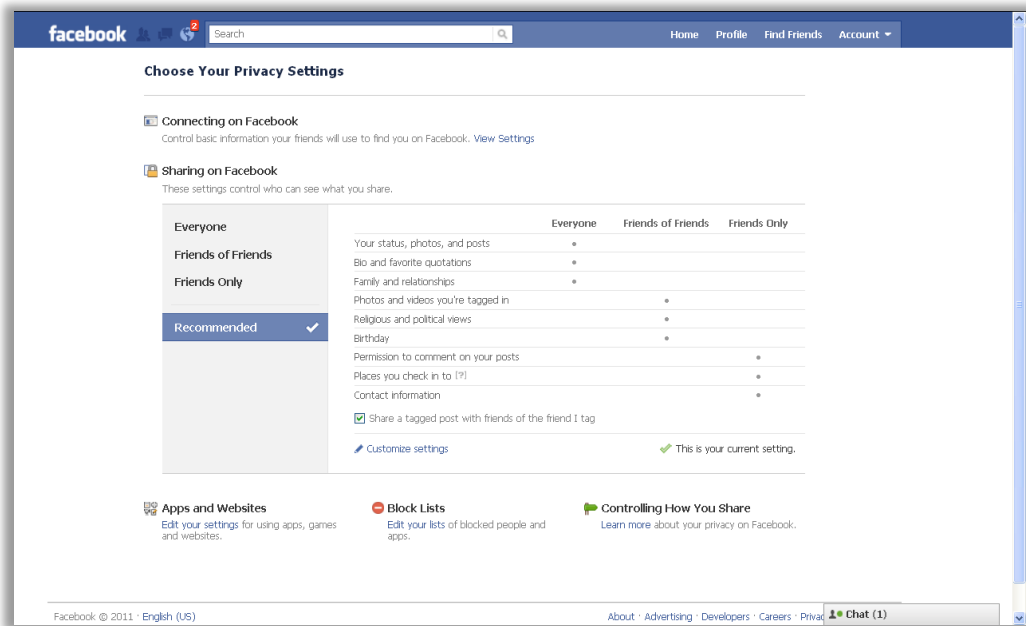


Figure 11- 09: Privacy Settings in Facebook



## Profile Settings

Users should set profile settings to be **“Only my friends.”** By default, Facebook allows all of the networks and all of users’ friends to be able to view their profile. Users are revealing personal information to potential identity thieves if they keep this option at default settings. Therefore, it is advised to set the profile to be viewed by only friends.

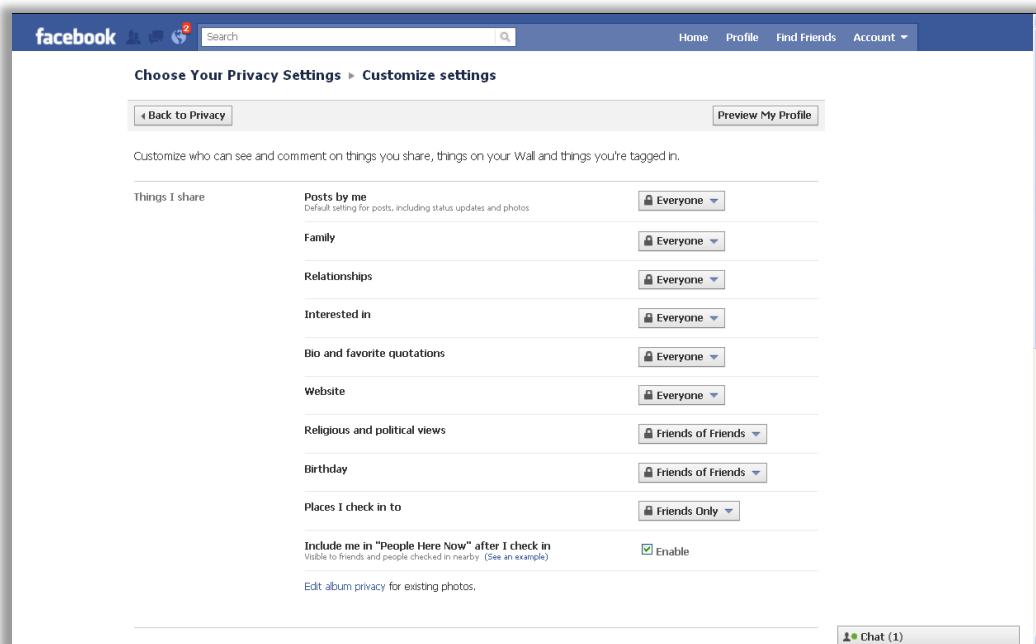


Figure 11- 10: Profile Settings in Facebook



## Privacy Settings for Applications

The privacy settings for applications control what **information** is **shared** with **websites** and **apps**, including search engines. A user can view your apps, remove any you do not want to use, or completely turn off the platform. Everybody on Facebook can read user notes, but it is advisable to **limit** notes **visibility** to just friends.

**Info accessible through your friends**

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

<input checked="" type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input checked="" type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input type="checkbox"/> Photos and videos I'm tagged in
<input type="checkbox"/> Religious and political views	<input checked="" type="checkbox"/> Hometown
<input checked="" type="checkbox"/> My website	<input checked="" type="checkbox"/> Current city
<input checked="" type="checkbox"/> If I'm online	<input checked="" type="checkbox"/> Education and work
<input checked="" type="checkbox"/> My status updates	<input checked="" type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My photos	<input type="checkbox"/> Places I check in to

Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

[Save Changes](#) [Cancel](#)

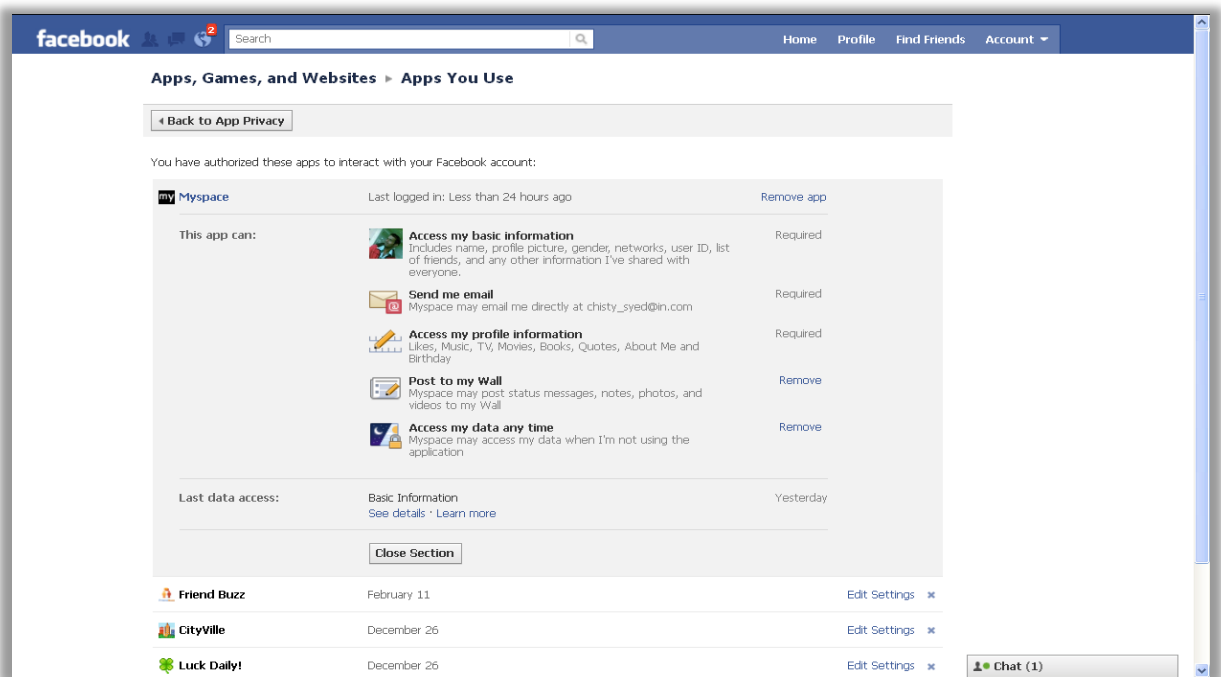
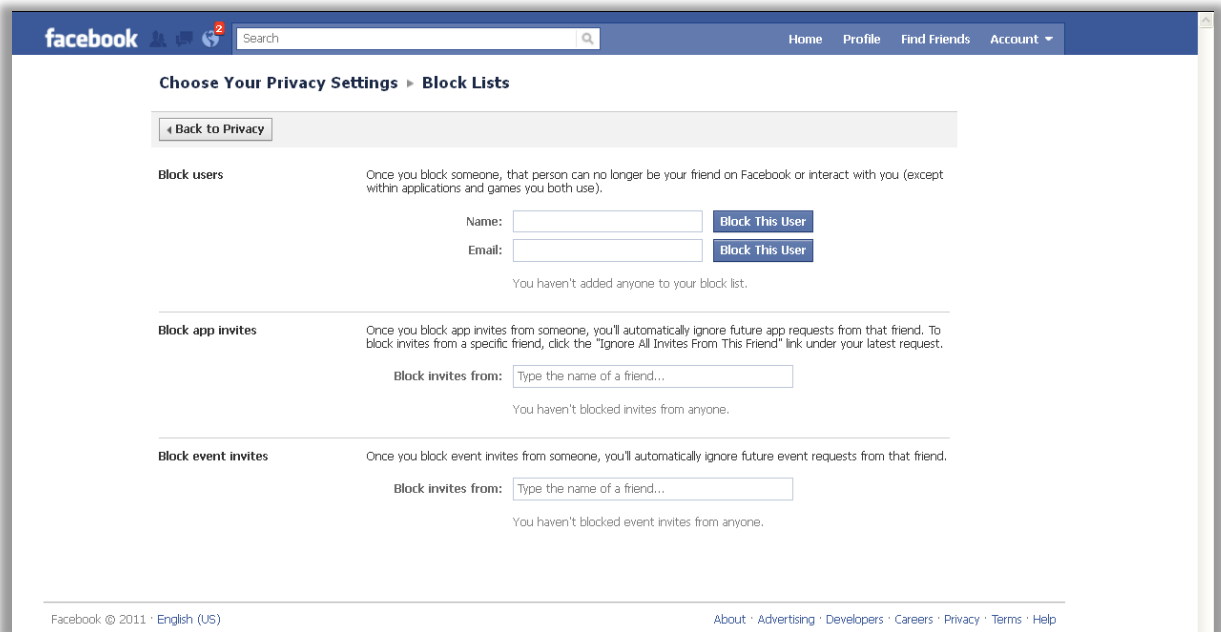


Figure 11- 11 Facebook Privacy Settings for Applications



## Settings to Block Users

This setting lets you block people from interacting with you or from seeing your information on Facebook. Users can also specify friends they want to **ignore app invites** from, and see a list of the specific apps that they've blocked from accessing their information and contacting them.



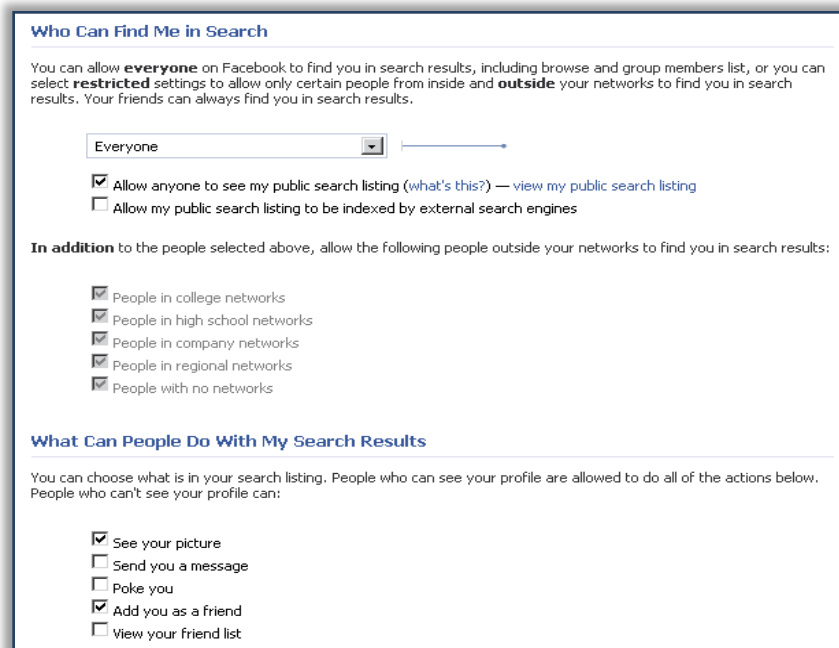
The screenshot shows the Facebook 'Block Lists' settings page. At the top, there's a navigation bar with 'facebook' logo, a search bar, and links for 'Home', 'Profile', 'Find Friends', and 'Account'. Below the navigation bar, the page title is 'Choose Your Privacy Settings > Block Lists'. A 'Back to Privacy' button is on the left. The main content area is divided into three sections: 'Block users', 'Block app invites', and 'Block event invites'. Each section has a brief explanation of what blocking does and a form to add someone to the block list. The 'Block users' section has fields for 'Name' and 'Email', each with a 'Block This User' button. The 'Block app invites' and 'Block event invites' sections have a 'Block invites from:' field with a placeholder 'Type the name of a friend...' and a 'Block This User' button. At the bottom, there's a footer with 'Facebook © 2011 · English (US)' and links for 'About', 'Advertising', 'Developers', 'Careers', 'Privacy', 'Terms', and 'Help'.

Figure 11- 12 Facebook Block User Settings



## Recommended Actions for Facebook Search Settings

Users should **restrict** who can find them in search results. Selecting everyone allows all Facebook users to find the user in search results.



The screenshot shows the Facebook 'Who Can Find Me in Search' settings page. The title is 'Who Can Find Me in Search'. Below the title, there's a paragraph explaining that users can allow everyone to find them or restrict settings to allow only certain people from inside and outside their networks. A dropdown menu is set to 'Everyone'. Below the dropdown, there are two checkboxes: 'Allow anyone to see my public search listing (what's this?) — view my public search listing' (checked) and 'Allow my public search listing to be indexed by external search engines' (unchecked). Below these, there's a section titled 'In addition to the people selected above, allow the following people outside your networks to find you in search results:'. This section has five checkboxes, all of which are checked: 'People in college networks', 'People in high school networks', 'People in company networks', 'People in regional networks', and 'People with no networks'. Below this, there's a section titled 'What Can People Do With My Search Results'. This section has a paragraph explaining that users can choose what is in their search listing and that people who can see their profile are allowed to do all of the actions below. There are five checkboxes: 'See your picture' (checked), 'Send you a message' (unchecked), 'Poke you' (unchecked), 'Add you as a friend' (checked), and 'View your friend list' (unchecked).

Figure 11- 13: Search Settings in Facebook

### Recommended Actions for Facebook “Search Settings”:

Option	Recommended Action	Reason
Allow anyone to see my public search listing	Be careful	The users should select the option “Yes” only if they want people they are familiar with to know that they are on Facebook.
Allow my public search listing to be indexed by external search engines	“No”	If enabled, this setting allows people using external search engines, such as Google, Yahoo, and MSN to find the user on Facebook.
See your picture	Be careful	The users should not share pictures that may embarrass them or are personal.
Send you a message	“No”	If users respond to a message sent by someone that they are not friends with, the unknown users will be able to view the user’s profile.
Poke you	“No”	By responding to the poke from an unknown user, users will be allowing him or her to view their profile information for a period of time.
Add you as a friend	Be careful	Be cautious before accepting anyone’s friend request.
View your friend list	“No”	The user should not allow people who are not yet their friends to view their friend list.

**Table 01: “Search” Setting Table**



### Facebook: Security Tips

The following are a few security tips that users should follow to stay safe on Facebook:

- Adjust Facebook **privacy settings** to help protect identity
- Think carefully** about who is allowed to become a friend
- Show “limited friends”—a cut-down version of the profile
  - Facebook allows its users to make people “limited friends,” which gives only partial access to a user’s profile
  - This is useful if the users have connections with whom they do not feel comfortable sharing personal information with
- Enable access** to information **only when necessary**



## Staying Safe on MySpace

The following steps allow users to stay safe on the social networking site, “MySpace”:

### Step1:

- Go to **Account Settings**, and click **Privacy**.
- Do not check **Online Now** if you do not wish others to know when you log in.
- Check **Show my birthday to my friends** only if necessary.
- Check the following options under applications:
  - Do not allow my profile information to be accessed by games and third-party services I haven’t connected to
  - Do not allow communications from games and third-party services I haven’t connected to

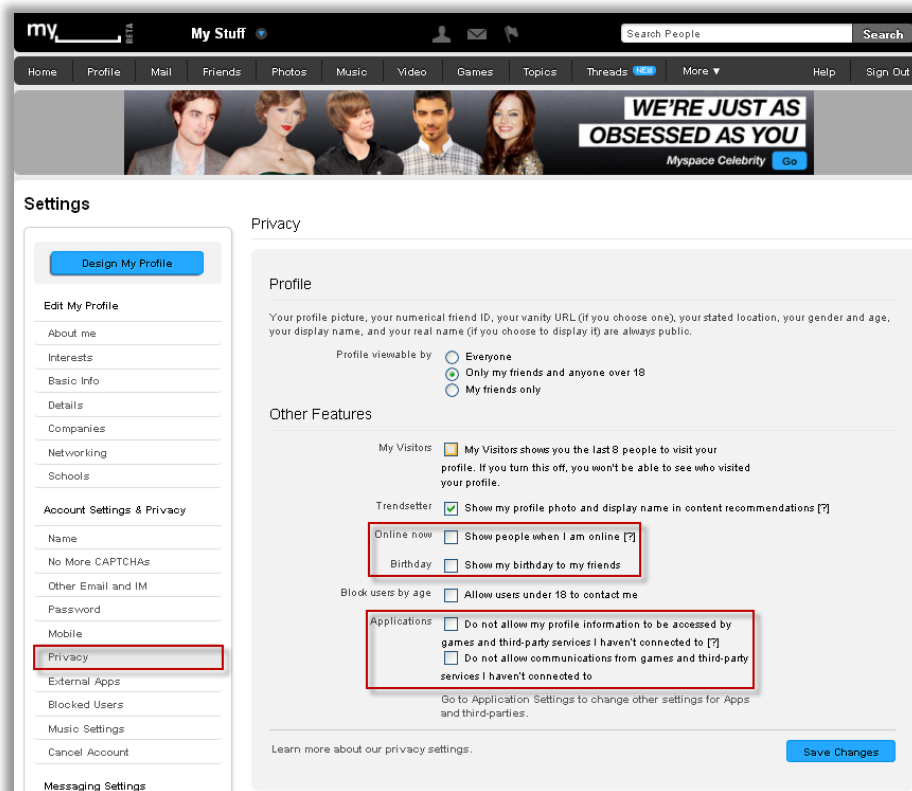


Figure 11- 14: MySpace Account Settings

### Step2: Check Settings for “Comments” and “Mail”

- Go to **Account Settings** → **Comments** and check **Only Friends can add comments to my blog**.
- Go to **Account Settings** → **Mail** and check **only people I know** to receive emails only from people you know.



**Comments**

☐ Require approval before comments are posted

☐ Require CAPTCHA [?] from users suspected of spamming

☒ Only Friends can add comments to my blog

[Save Changes](#)

---

**Mail**

**Messages**

☐ Allow non-friends to send me new messages

☐ Require CAPTCHA [?] for non-friends to send me messages

**Privacy**

Who can email me ☐ Open  
Don't worry, spam will be filtered

☒ Only people I know  
Only Myspace friends and address book contacts - [Import contacts](#)

**Figure 11- 15: MySpace Comments and Mail Settings**

**Step3:** Check the following settings for **Friends Request** and **IM**

#### **Friends Request Settings**

- ➊ Go to **Account Settings** → **Friends Request**.
- ➋ Check **Require CAPTCHA [?] from users suspected of spamming** and also check other options according to your preferences.

**Friend Requests**

☒ Require CAPTCHA [?] from users suspected of spamming

☐ Allow bands to send friend requests

☐ Allow comedians to send friend requests

☐ Allow filmmakers to send friend requests

[Save Changes](#)

**Figure 11- 16: MySpace Friend Request Settings**

#### **IM Settings**

- ➌ Go to **Account Settings** → **IM**.
- ➍ Check **Only my IM friends** to appear only in friends' IM lists.

Privacy

Want to specify which of your friends will appear in your IM list?. [Edit IM friends.](#)

Who can see me on IM ☐ Everyone  
☐ All my IM and Myspace friends  
☒ Only my IM friends

[Save Changes](#)

**Figure 11- 17: MySpace IM Settings**

**Step4: Check Settings for Stream Settings**

- ➊ Go to **Account Settings** → **My published activities** and check the proper option according to your preferences.
- ➋ Go to **Account Settings** → **My Friends' Activities** and check the proper option according to your preferences.

My published activities

Update Stream with the following activities:

- ☒ Profile (update any profile sections such as interests, details, schools, or contact information)
- ☒ Photos (upload photos, tag photos)
- ☐ Video (upload video, favorite a video, etc)
- ☐ Games (install a game, reach an achievement in a game etc)
- ☐ Music (add a song to playlist, upload a karaoke song)
- ☒ Bulletins (post a bulletin)
- ☒ Blog (post a blog)
- ☐ Events (create an event, RSVP to an event)
- ☐ Topics and Hubs
- ☒ Threads
- ☒ Misc
- ☒ Comments (advanced options)

My Friends' Activities

Update Stream with these activities from my friends:

- ☒ Profile (update any profile sections such as interests, details, schools, or contact information)
- ☐ Photos (upload photos, tag photos)
- ☒ Video (upload video, favorite a video, etc)
- ☒ Games (install a game, reach an achievement in a game etc)
- ☒ Music (add a song to playlist, upload a karaoke song)
- ☐ Bulletins (post a bulletin)
- ☐ Blog (post a blog)
- ☒ Events (create an event, RSVP to an event)
- ☒ Topics and Hubs
- ☐ Threads
- ☒ Misc
- ☐ Comments (advanced options)

**Figure 11- 18: MySpace Stream Settings**

**Step 5: Settings for Block Users by Age**

- ➌ Do not check **Allow users under 18 to contact me.**
- ➍ Checking this option would allow all the fake users who pose as under 18 to access your account
- ➎ To deny any unauthorized access to the profile, block the user by adding their profile URL to the blocked users' list.

Block users by age ☐ Allow users under 18 to contact me

---

Block a user via profile URL:  [Block](#)

---

Unblock User After you unblock a user, he or she will be able to send you friend requests and messages.

**Figure 11- 19: MySpace Block Users by Age Settings**



## Module Summary

Social networking websites allow users to build online profiles, share information, pictures, blog entries, music clips, etc.

A user's main profile page on any social networking site introduces and describes the user.

Cyber bullying is the process of using technology to harass or bully someone.

Social networking sites contain users' information like email addresses and archived messages that can be used to customize email messages or fake websites

Malware attacks are carried out through social engineering as users are mostly misled into clicking malicious links embedded within personal messages.

Set appropriate privacy and security defaults and choose a complex/unique password for the account.



## Social Networking Security Checklist

The following is a list of the best practices a user should follow for Social Networking Security:

- ☐ Choose a complex/unique password for the account
- ☐ Read the privacy policy and terms of service carefully
- ☐ Do not post anything personal on the social networking site
- ☐ Set appropriate privacy and security defaults to make your profile private
- ☐ Be careful about what is posted on the Internet
- ☐ Be careful installing third-party applications
- ☐ Only accept friend requests from people you know
- ☐ Only share limited personal information



## **Social Networking Security Checklist**

The following is a list of the best practices a user should follow for Social Networking Security:

- ☐ Apply privacy settings so that only friends can view your profile information
- ☐ Do not use common verification such as your date of birth or your mother's maiden name
- ☐ Be aware of the intentions of anyone you meet on these sites
- ☐ Restrict the access of personal videos on social networking sites to friends
- ☐ Disable the comments to prevent cyber bullying
- ☐ Do not click suspicious links to prevent malicious attacks
- ☐ Update the computer with the latest antivirus and other system security software
- ☐ Never install codecs when a site prompts you to do so



## **Social Networking Security Checklist for Parents and Teachers**

The following is a list of the best practices a Parents and Teachers should follow for Social Networking Security:

- ☐ Be open with kids; encourage and instruct them to seek permission before providing any details on social networking sites
- ☐ Read the privacy policies of the sites before allowing children to use them
- ☐ Consider keeping the computer in a family room rather than the child's bedroom
- ☐ Instruct children to never respond to messages that are suggestive, obscene, belligerent, threatening, or make them feel uncomfortable
- ☐ Create your own account on the social network and spend some time on the network's site to familiarize with social networking media
- ☐ Create a cheat sheet with your child's password, a list of his/her approved friends, and rules for how your child operates
- ☐ Know children's passwords, screen names, and account information; this will help in monitoring their activities
- ☐ Instruct your child to add people to their "friends" list only if they know them in real life