Cyberstalking

Cyberstalking has been defined as the use of information and communication technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals or organisation.
The behaviour includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment and gathering information for harassment purposes.

Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behaviour that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

How Stalking Works ?

It is seen that stalking works in the following ways :

1. Personal information gathering about the victim: Name, family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favours or threaten the victim.

If you are a victim of stalking, consider suspending your social networking accounts until the stalking has been resolved. If you decide to continue to use social networking sites, here are a few tips to help keep you safe:

- Take advantage of privacy settings. With some social networking sites, you may be able to make your profile completely private simply by checking a box. With others, such as Facebook, privacy settings can be complex to navigate.
- Take advantage of added security settings. One of the best examples is two-factor authentication. When you enable this, your account will require you to provide something you know (like a password) with something you have (like a specific device). Therefore, if someone gets your password, he or she will not be able to log in to the account without the specific code that the service sends to your device

- Limit how much personal information you post to your account. For example, you may not want to include contact information, your birth date, the city you were born in or names of family members.
- Do not accept "friend requests" (or "follow requests") from strangers. If you recognize the individual sending the request, contact him or her off-line to verify he or she sent the request.
- Warn your friends and acquaintances not to post personal information about you, especially your contact information and location.
- Avoid online polls or quizzes, particularly those that ask for personal information.
- Don't post photographs of your home that might indicate its location. For example, don't post photographs showing a house number or an identifying landmark in the background.
- Use caution when joining online organizations, groups or "fan pages." Never publicly RSVP to events shown online.
- Use caution when connecting your cell phone to your social networking account. If you do decide to connect your cell phone to your online account, use extreme caution in providing live updates on your location or activities.
- Avoid posting information about your current or future locations, or providing information a stalker may later use to hone in on your location, such as a review of a restaurant near your house.
- Always use a strong, unique password for every social networking site.

SQL Injection

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statement or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Attackers target the SQL servers - common database servers used by many organizations to store confidential data. The prime objective behind SQL injection attack is to obtain the information when accessing a database table that many contain personal information such as credit card numbers, social security numbers or passwords. During an SQL injection attack, Malicious Code is inserted into a web form field or the website’s code to make a system execute a command shell or other arbitrary commands. Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field. For example, an arbitrary command from an attacker might open a command prompt or display a table from the database. This makes an SQL sever a high-value target and therefore a system seems to be very attractive to attackers.

The attacker determines whether a database and the tables residing into it are vulnerable, before launching an attack. Many webpages take parameters from web user and make SQL query to the database. For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password. With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback etc. The attackers also looks for the webpages that display the HTML commands such as POST or GET by checking the site’s source code.
2. To check the source code of any website, right click on the webpage and click on “view source” (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML and look for “FORM” tag in the HTML code. Everything between the <FORM> and </FROM> have potential parameters that might be useful to find the vulnerabilities.

   ```
   <FORM action=Search/search.asp method=post>
   <input type=hidden name=A value=C>
   </FORM>
   ```
3. The attacker inputs a single quote under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as *use “a” = “a”* (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**
    - Replace all single quotes (escape quotes) to two single quotes.
    - Sanitize the input: User input needs to be checked and cleaned of any characters or strings could possibly be used maliciously. For example, character sequences such as ; ,--,select, insert and xp_ can be used to perform an SQL injection attack.
    - Numeric values should be checked while accepting a query string value. Function IsNumeric( ) for Active Server Pages (ASP) should be used to check these numeric values.
    - Keep all text boxes and form fields as short as possible to limit the length of user input.
2. **Modify error reports:** SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error reports very carefully. These errors some time display full query pointing to the syntax error involved and the attackers can use it for further attacks.
3. **Other preventions**
    - The default system accounts for SQL server 2000 should never be used.
    - Isolate database server and web server. Both should reside on different machines.
    - Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc. then these should be moved to an isolated server.