International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 4 : Issue 3 *[ISSN 2250 – 3757]*
Publication Date : 30 September, 2014

Internet Safe Browsing Awareness to Prevent Cyber Attacks

Vanika Makhija*, Radha Adhikari*, R.H.Goudar**

***Abstract*— Preservation of confidentiality, integrity and availability of information in the cyberspace is Cyber Security. It is a complex issue that cuts across multiples domains calls for multidimensional, multilayered initiatives and responses. It is necessarily important to stop cyber crime and raise greater public awareness of the steps of every person. As our nation rapidly building in Cyber-Infrastructure, it is equally important that we educate our population to work properly with this infrastructure. This paper deals with the basic awareness for people who are browsing and some of the solutions to prevent cyber attack and also security to his credentials. Also it tells us the various tools and applications available, to protect individual and their information to ensure confidence in online experience.**

Keywords*— Keylogger Spyware, 2-step verification, Phishing, Virtual Keyboards, Social sites.

Introduction

Cyber crime is one of the largest illegal industries in the world. It is criminal activity, using computers and the Internet to steal, whether directly or indirectly, from consumers or businesses. Cyber criminals may use computer technology to access personal information, business trade secrets or use the internet for explotive or malicious purposes. Cyber-security is a challenge that extends beyond national boundaries and requires global cooperation with no single group.

Cyber security is the activity of protecting information and information systems (networks, computers, databases, data centers and applications) with appropriate procedural and technological security measures. Firewalls, antivirus software and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security.

Awareness is commonly used in reference to public knowledge or understanding of social or political issues.

- Security awareness will help employees to understand how to make workplace more secure.
- It teaches skills to protect yourself and family from cyber crime and identity theft.

Vanika Makhija* , *Radha Adhikar**
Dept. of CSE, Graphic Era University,
Dehradun, India

*R H Goudar***
Dept. of Computer Network Engineering (CNE),
Visvesvaraya Technological University (VTU),
Belgaum-590018, India

I. Security on social sites

A. *Facebook*

Facebook privacy shortcuts give you quick access to some of the most widely used privacy settings and tools.

Some of its features are:

- Click at the top right of the page to see shortcuts that help you manage and click on the privacy setting.(Fig:1.1 & 1.2)

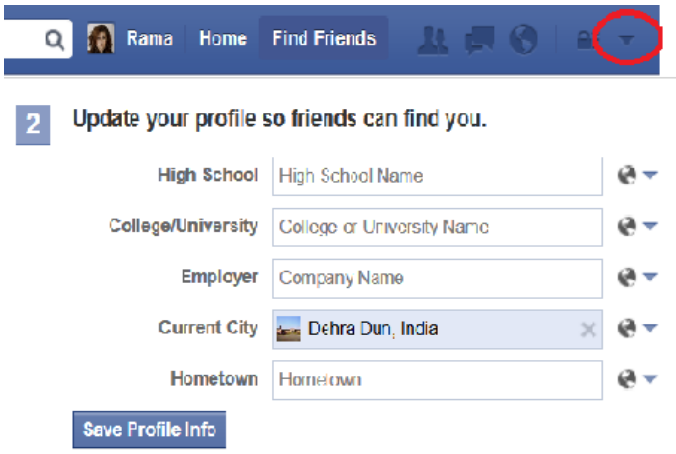


Fig: 1.1 Snapshot of Facebook Privacy shortcuts

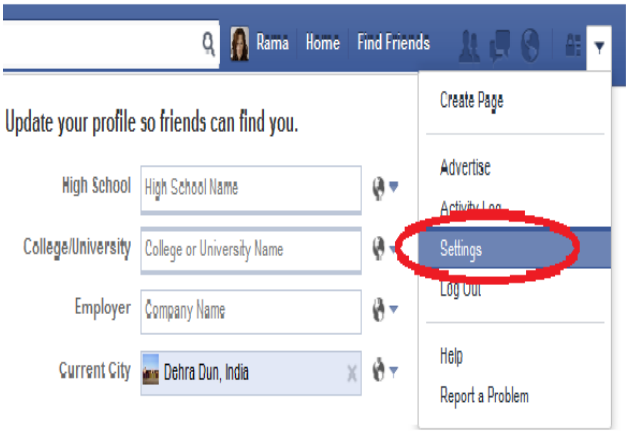


Fig: 1.2 Snapshot of Facebook Account settings menu

- Under those settings we can control whether who can see our stuff and customize it according to our choice.(Fig:1.3)

.

- Also under security settings there is an option to know if our account is accessed from a new device or computer and get a text message.(Fig:1.4)

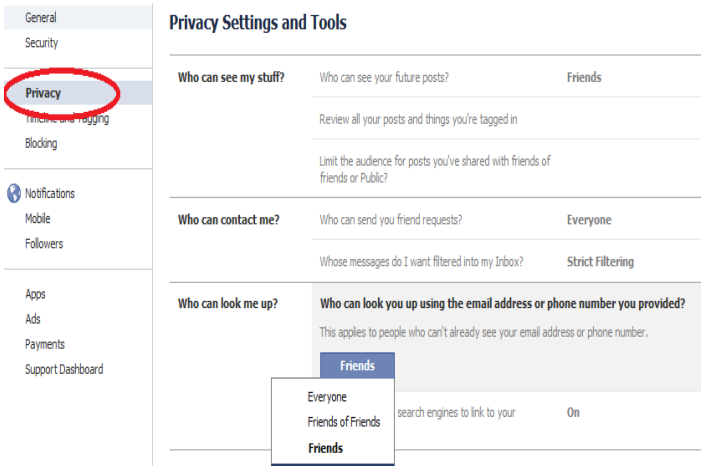
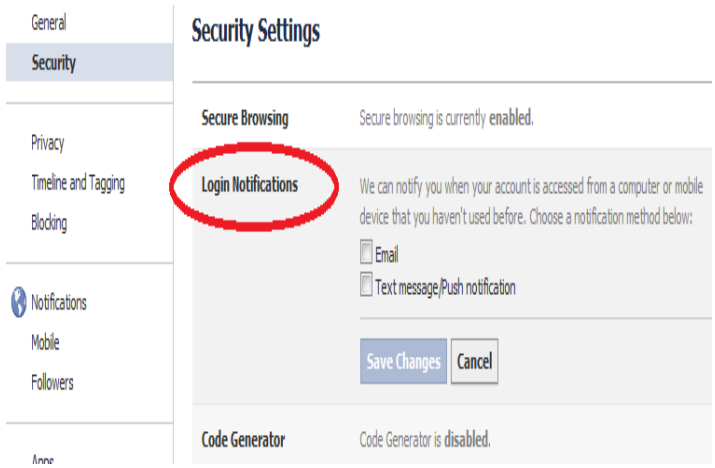


Fig: 1.3 Snapshot of Facebook Privacy settings and tools



` Fig:1.4 Snapshot of Security settings on Facebook

Secure browsing (https) is a security feature. When you have secure browsing turned on, they will encrypt your activity on Facebook where possible, making it harder for anyone else to access your Facebook information without your permission.

B. *Twitter*

Use login verification

Login verification is a feature that helps you keep your account more secure. Instead of relying on just a password, login verification introduces a second check to make sure that you and only you can access your Twitter account.

1. Click on the gear icon in the upper right and under those select the settings option.(Fig;2.1)

2. Select the security and privacy tab.(Fig:2.2)

3. Under those settings you can select option to send login verification of your account.

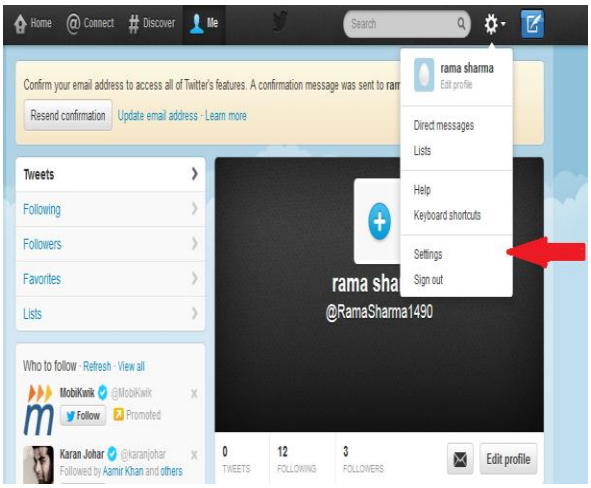


Fig: 2.1`Twitter security and privacy tab

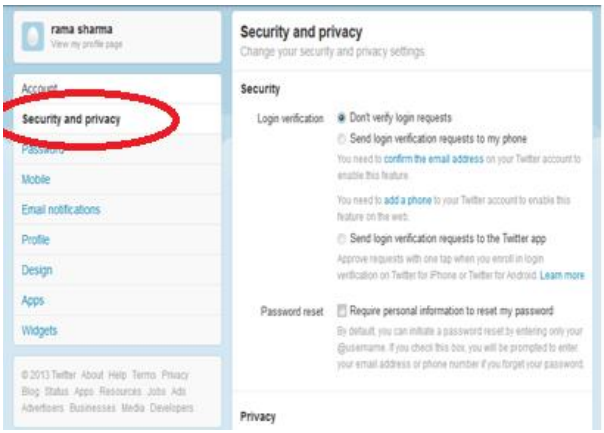


Fig:2.2 Twitter security and privacy menu

C. *Linkedin*

We can select what others see when they view our profile from the Privacy & Settings page. There are three different ways we show information on who's viewed your profile, based on the profile viewer's privacy settings.(Fig:3.1)

- Display viewer's name, headline, location and industry.

- Display only anonymous profile characteristics such as job title, company, school, and industry.

- Display as an anonymous LinkedIn Member. This reflects members who have viewed your profile and chose to remain anonymous.

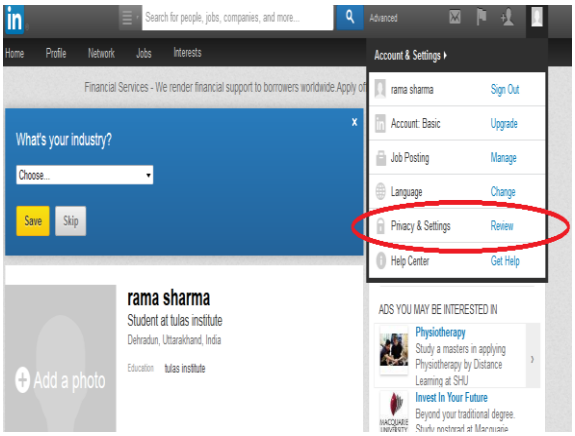


Fig: 3.1 LinkedIn Account settings tab

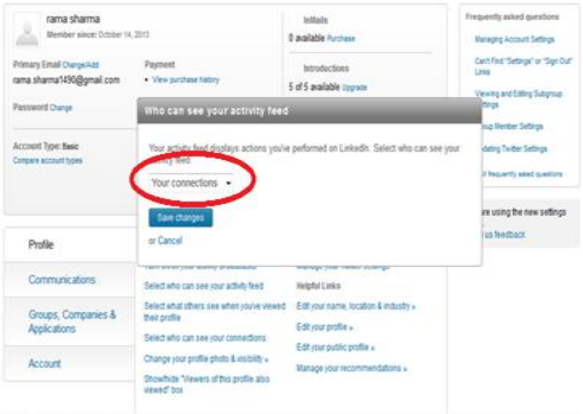


Fig: 3.2 LinkedIn Privacy setting menu

II. Email Accounts

GMAIL

Google has offered a 2-step verification system, which is a bullet proof security thing for GMAIL accounts.(Fig:4.1)

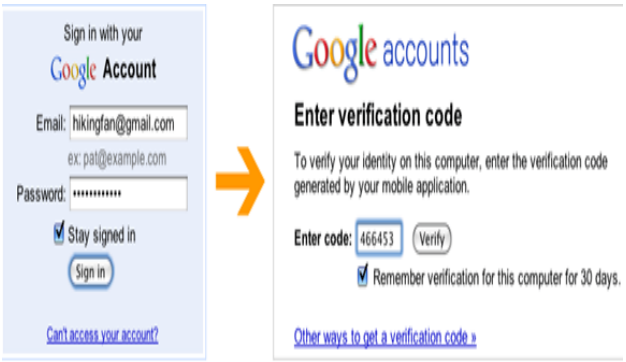


Fig: 4.1 Snapshot of 2-step verification security option

Steps to enable this security option:

1. Open the "Account Page" and you will see this option under Personal Settings.

2. 2. Click on the "**Using 2-step verification" link and it may ask you to enter your Gmail account password**.(Fig:4.2)

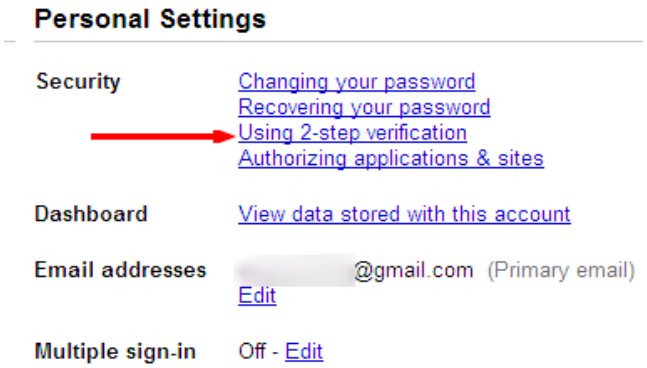


Fig: 4.2 Personal settings in Gmail account

3. After that you will see the 2-step verification setup page. Click the button **"Set up 2-step verification".** (Fig: 4.3)

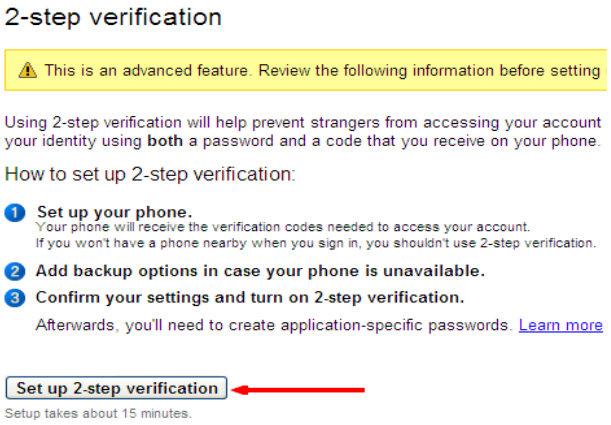


Fig: 4.3 2-step verification menu

4. On this Set up your phone page, enter the details and test your phone by clicking on the "**Send Code" button. You will receive a code via SMS or automated voice message (depends on your selection). Enter that code in the Code verification box and click "Verify"**(Fig:4.4)

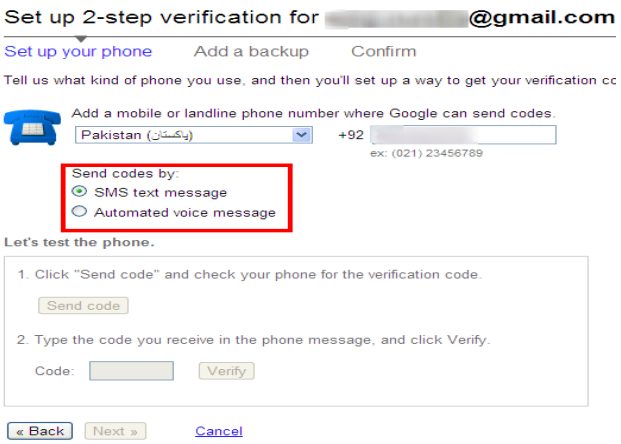


Fig:4.4 Option for receiving the code

- Enter the code and you can tick mark the box "**Remember verification for this computer". In this case, your verification code will be saved for this computer only for 30 days. Click "Verify" and you are now logged in.**(Fig: 4.5)

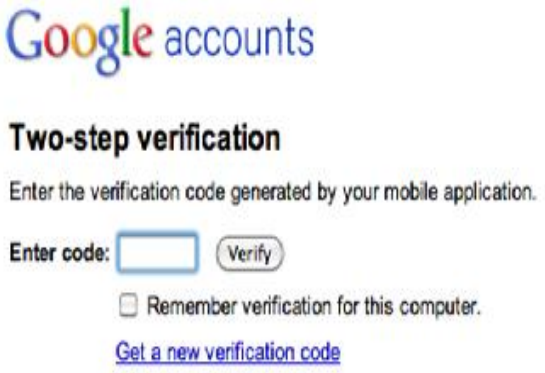


Fig: 4.5 Screen for entering the code

III. Protective Measures to be Taken

- It is recommended to type the full URL of bank's website yourself on the web-browser.
- Always go through your mailbox on the Internet Banking webpage after login and read carefully security alerts/messages sent by the Bank.
- User must monitor account activity regularly by checking the balances and statements online.
- Check for padlock icon, a de-facto standard, displayed somewhere on web-browser, representing the site's security certificate (Fig: 5.1)

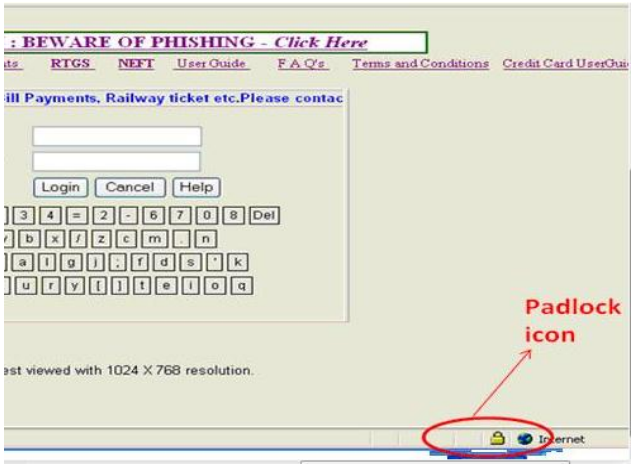


Fig:5.1 Padlock icon on browser page

- Click on icon to check the security certificate – address on the certificate conforms to the address in the address bar (Fig: 5.2)

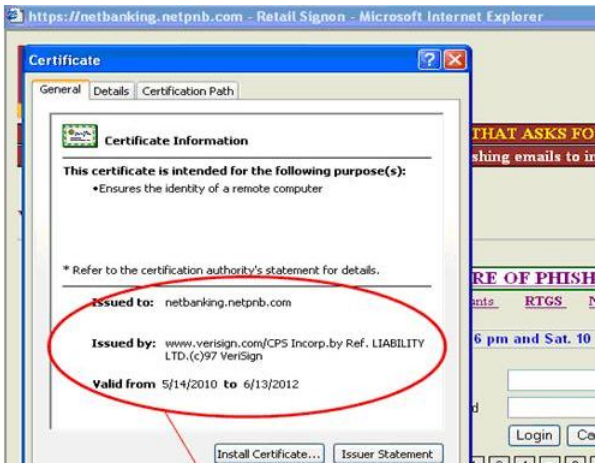


Fig: 5.2 Security certificate on address bar

- User must always check the last log-in in Internet Banking Account and if some unusual activity is noticed immediately contact bank.
- Mobile number should be register for SMS Alerts, for Internet Banking Transactions through ATM/Branches, for receiving alerts for specific transactions in your account.

IV. Protective Measures to be Taken

1. Get to your favourite social media sites by typing in the exact address into your browser.

For eg: a site with extension ".com" is very different from other site with the same domain name but different extension that is ".in"(Fig: 6.1)

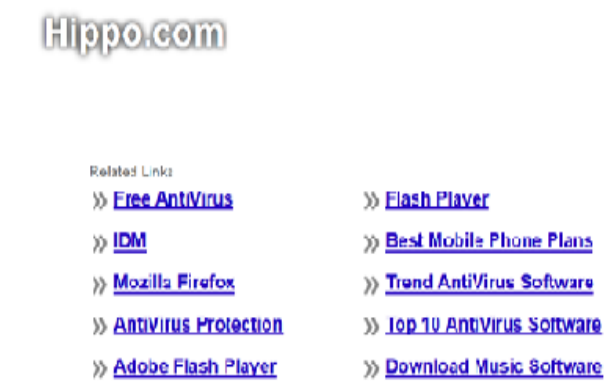


Fig: 6.1 Snapshot of site with extension ".com"

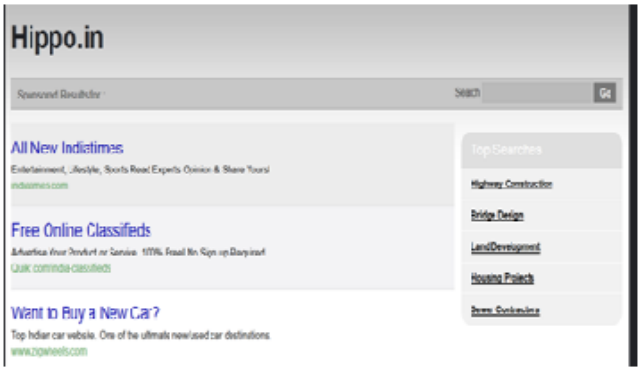


Fig: 6.2 Snapshot of site with extension ".in"

2. Never go in through an email link or via another website to reach it because it could be a trap to get your account name and password.(Fig: 6.3)

It's not uncommon for a unsuspecting employee to click on a link or download an attachment that they believe is harmless -- only to discover they've been infected with a nasty virus, or worse. As such, never click on a link that you weren't expecting or you don't know the origination of in an e-mail. You have to "be smart when surfing the Web, should take every "warning box" that appears on screen seriously and understand that every new piece of software comes with its own set of security vulnerabilities.

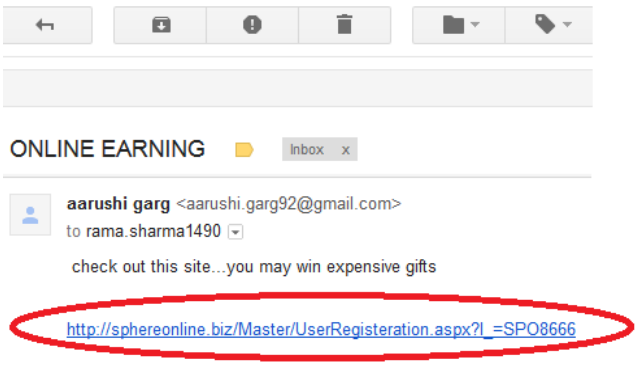


Fig: 6.3 Email link on gmail account

When visiting a site, and logging in, look for the padlock icon. This is an indication that the site is authenticated and encrypted, protected by means of Transport Layer Security

v. Keylogger Spyware Attack

A keylogger is a software program designed to secretly monitor and log all keystrokes.A kelogger spyware is a combined script attack,contains both scripts keylogger and spyware in a single program.A keylogger which captures all keystrokes in a log file and other is spyware which emails this to hacker's specified address.Many keylogger hide themselves in a system.Unlike mailicious program,keylogger present no threat to system.they can be used to intercept passwords or confidential information entered through keyboard.
They can be divided into two categories:

- KEYLOGGING DEVICES:small devices that can be fixed to the keyboard or placed within cables.
- KEYLOGGING SOFTWARE:dedicated programs designed to track and log keystrokes.

HOW TO KNOW IF WE HAVE A KEYLOGGER:

- **Monitor the behaviour of PC**: Slow computer performance, new icons on desktop, unexpected pop-ups adds to these symptoms. Also you can notice that the text that you type can appear with little delay – this is the direct symptom that will help you in keystroke logger detection.
- **Verify process threads**:Computer keep records of all our running threads.
  To view our running thread:
  1.Press CTRL+ALT+DELETE, and then select Task Manager in the menu.
  2.Select Processes tab, scroll the list. Find the process that is called winlogon.exe. One process with such a name is a normal thing, but if you have 2 processes with the same name, then you have a Keylogger.
  3.Highlight the second winlogon.exe and click End process (you should end only the second process with such a name**)**(Fig: 7.1)

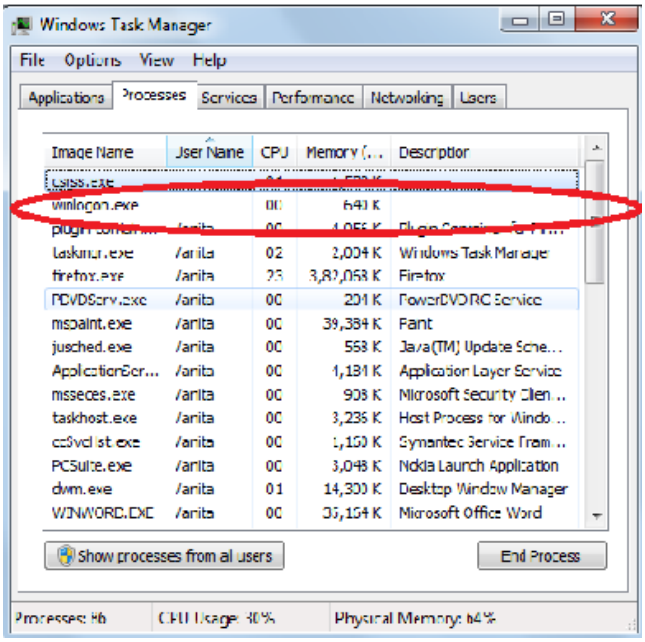


Fig: 7.1 Windows task manager Screen

- You can also detect this malicious program with the help of **Startup** list. So, you should follow the instructions:
  1.Press **Windows+R** buttons, then type **'msconfig'** in the line and press Enter.
  2.Select **Startup** tab and disable all the **unknown programs.**
  3.Then restart your computer.

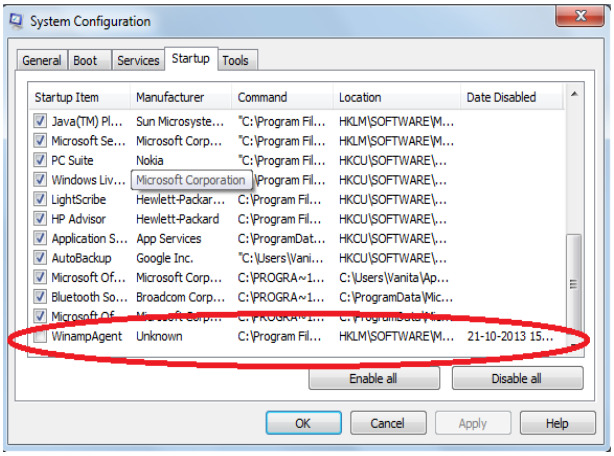


Fig: 7.2 System configuration settings

- Check the list of installed programs for anything unfamiliar or suspicious(Fig: 7.2)
- Perform visual check on computer's hardware,keylogger be a piece of hardware attached to computer

VI. PHISING ATTACK

A phishing attack involves use of web site that has been set up by criminals to look like websites of well known organization. When internet fraudsters impersonate a business to trick us into giving our personal information**.**

- **Phishing email**: The attacker sends a spam email to thousands of email addresses pretending to be from a legitimate organization. The email is worded to persuade the user to click on a link in the email. If the user clicks on the link, the user's computer will connect to the phishing web site.
- **Phishing web site**: The phishing web site is created to capture any fields completed by the user (such as username and passwords). If the user completes these fields the information will be captured by the attacker.

A. *How to Protect:*

The best way to avoid becoming a victim of a phishing attack is to detect and/or block the phishing email.

- Use a spam filter to block spam email. By blocking and filtering spam email, users are less likely to read, trust or click on a link in a phishing email.
- Change settings on your email software to warn you when you receive a suspicious email that may be a phishing email.

For eg:
1.In Microsoft Internet Explorer version 7, the phishing filter can be turned on by selecting "Tools" menu, then "Internet Options", then select "Turn on automatic website checking"(Fig: 8.1)

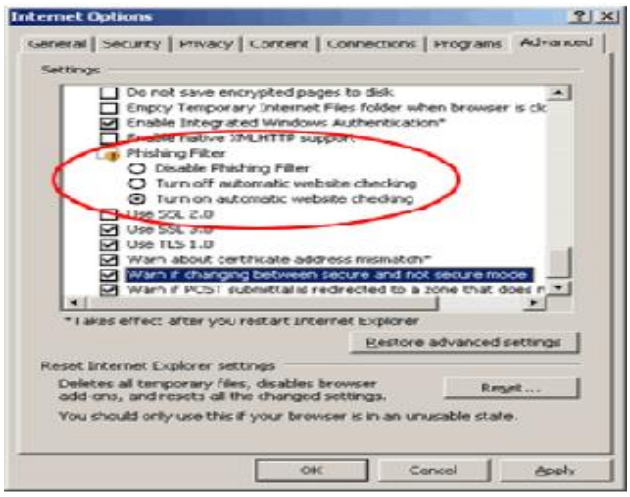


Fig: 8.1 Microsoft Internet Explorer tools menu

2.Click "Apply" then "OK" to save these settings.

3.In Microsoft Internet Explorer version 8, anti-phishing is handled by the SmartScreen Filter. The SmartScreen Filter is enabled by default - you can confirm that it is enabled by selecting the "Safety" menu, then "SmartScreen Filter".(Fig:8.2)

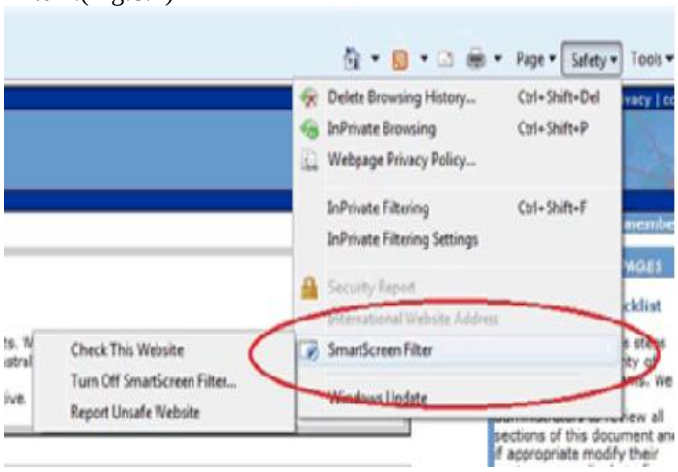


Fig: 8.2 Smart Screen Filter on Microsoft Internet Explorer

- In Mozilla Firefox, click on Tools menu, select Options, select the Security tab then select the check box for "Tell me if the site i'm visiting is a suspected forgery". Either option is fine, however, according to the Mozilla Firefox help notes, the Google option will provide a more reliable check for you.(fig: 8.3)

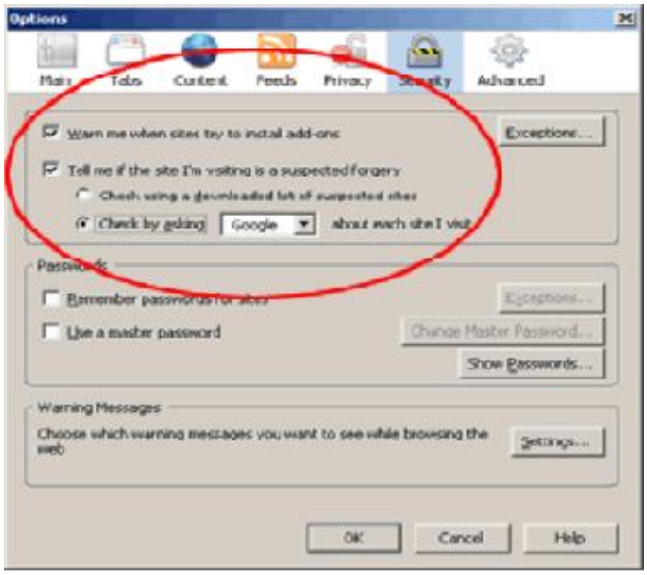


Fig: 8.3 Mozilla Firefoz tools menu

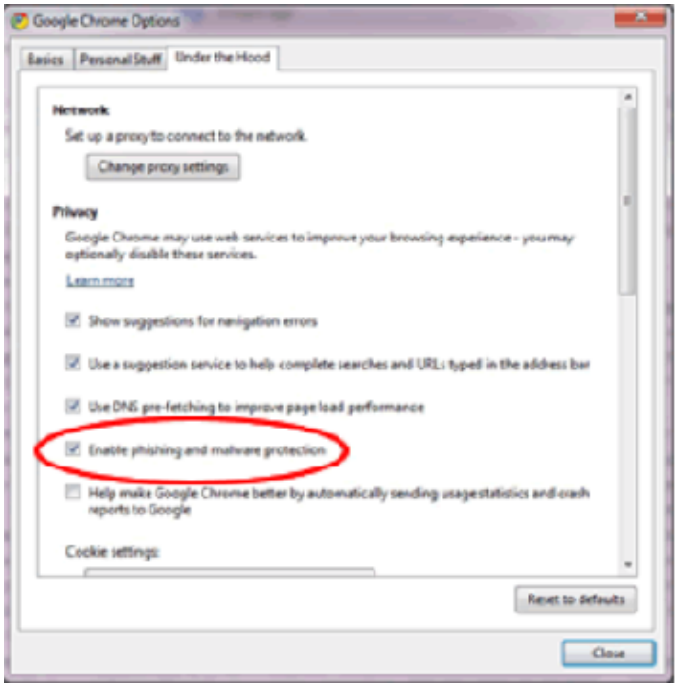


Fig: 8.4 Google Chrome customise settings

- In the Google Chrome web browser, phishing and malware protection is enabled by default. Confirm this by selecting the menu with a spanner icon (rolling over this menu will display the text "Customize and control Google Chrome") and then "Options".(fig: 8.4)

B. *Typical Steps of a Phishing Attack*

In most phishing attacks, the user opens an email, and then clicks on a link in that email. This results in the user's browser getting exploited. Maybe there is also a form on the web page

that captures the users credentials as they are typed in. Alternately, the user could open an email attachment and their machine gets compromised that way.

How does phishing email message look like?

Here is an example of what a phishing scam in an email message might look like.(Fig.8.5)

Fig: 8.5 [11] View of phishing email message

- Spelling and bad grammar**.** Cyber criminals are known for their grammar and spelling.

- Beware of links in email. If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.(Fig: 8.6)

Fig: 8.6 [11] Masked email link

- Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- Another common technique that has been used is a URL that at first glance is the name of a well-known company but on closer scrutiny is slightly altered. For example, www.microsoft.com could appear instead as:

www.micosoft.com

www.mircosofl.com

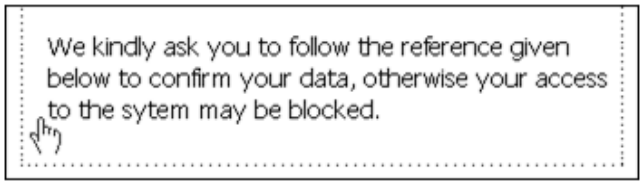


Fig: 8.7 [10] Detection of a fake email

- **Message body is an image** To avoid detection by spam filters, fake e-mail messages used in phishing schemes often use an image instead of text in the message body. If the sent spam message uses real text, the Outlook Junk E-mail Filter will very likely move the message to the **Junk E-mail** folder. The message body image is usually a hyperlink. You can tell because when you rest the pointer on the message body, the pointer becomes a hand.(fig:8.7) When you open the e-mail message the images are downloaded and information is passed back to the server. This information is used to verify that your e-mail address is valid and so you might be spammed again.
- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cyber criminals often use threats that your security has been compromised.

C. *Virtual Keyboard*

Virtual keyboards(fig:9.1) are commonly used as an on-screen input method in devices with no physical keyboard, where there is no room for one, such as a pocket computer, personal digital assistant(PDA), tablet computer or touch screen equipped mobile phone. It is common for the user to input text by tapping a virtual keyboard built into the operating system of the device. Virtual keyboards are also used as features of emulation software for systems that have fewer buttons than a computer keyboard would have. Virtual keyboards can be categorized by the following aspects:

- Physical keyboards with distinct keys comprising electronically changeable displays integrated in the keypads

- Virtual keyboards with touch screen keyboard layouts or sensing areas.
- Optically detected human hand and finger motions
- Virtual keyboards to allow input from a variety of input devices, such as a computer mouse, switch or other assistive technology device.(Fig: 9.1)

Fig: 9.1 Snapshot of virtual keyboard

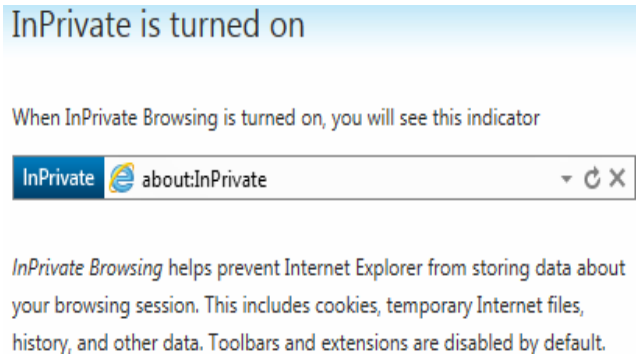


Fig: 9.2 Privacy Mode on Internet Explorer

Privacy Mode: Web browsers store information such as browsing history, images, videos and text within cache. In contrast, privacy mode can be enabled so that the browser does not store this information for selected browsing sessions.(fig: 9.2).

Give a fake password:

- If you are not sure if a site is authentic, don't use your real password to sign in. If you enter a fake password and appear to be signed in, you're likely on a phishing site
- Do not enter any more information. Close your browser.

Security Awareness Training:

Security awareness training helps you educate people to stop risky activities such as clicking on a link in a questionable email, opening an attachment they are not expecting, or submitting something on a bogus forum.

We can achieve this by:

1. Don't trust links in an email
2. Never give out personal information upon email request
3.Look carefully at the web address; it could be a close approximation of the real URL
4.Type the real website address into a web browser.
5.Don't call company phone numbers listed in emails or instant messages; check a reliable source such as a phone book or credit card statement
6.Don't open unexpected attachments or instant message download links
7. Be suspicious if emails says "do X or something bad will happen"
8.Be suspicious of any email with urgent requests for personal financial information
9.Always ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser; look for the https:// and/or the security lock icon.
10.Regularly log into your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate.
11.Enable two-factor authentication whenever possible. This combines something the user knows (such as a password or PIN) with something the user has (such as a smart card or token) or even something the user is (such as a biometric characteristic like a fingerprint).
12. Keep your operating system updated, ensure that your browser is up to date and security patches are applied
13. Always report "phishing" or "spoofed" e-mails to your IT department

Report phishing scams.**If you receive a fake phone call, take down the caller's information and report it to your local authorities. You can use Microsoft tools to report a suspected scam on the web or in email.**

- Internet Explorer**.** While you are on a suspicious site, click the gear icon and then point to **Safety**. Then click **Report Unsafe Website** and use the web page that is displayed to report the website.

- Outlook.com (formerly **Hotmail**). If you receive a suspicious email message that asks for personal information, click the check box next to the message in your Outlook inbox. Click the arrow next to **Junk** and then point to **Phishing scam**.

- Microsoft Office Outlook 2010 and 2013. Right-click the suspicious message, point to **Junk**, and then click **Report Junk**.

VII. Conclusion

With the advancement in technology there is increasing need of internet and its facilities, at the same time hackers are also becoming equally equipped. The growth of cyber crime all over the world is on the rise and to curb its scope and complexity is the pertinent need today. It is not possible to eliminate the cyber crime completely from the cyberspace, but it is possible to check them and this is possible only with the help of awareness about the various security threats. In this paper we presented the various security options available on the internet and also some of the methods to check if our system is not vulnerable to threats. There are several aspects of security which are covered and needs immediate attention but still there are numerous options available.

References

[1] Dale C. Rowe Ph.D. Barry M. Lunt PhD Joseph J. Ekstrom PhD Cyber theft: The Role of Cyber-Security in Information Technology Education.

[2] *Cyber Security* White *Paper* – Huawei:*www.huawei.com/ilink/en/download/HW_310547*

[3] Michael Barrett, Andy Steingruebl, Bill Smith April 2011:COMBATING CYBERCRIME Principles, Policies, and Programs

[4] Emerging Cyber Threats, Report for 2009: Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and beyond.

[5] *Keyloggers*: How they work and how to detect them:*www.securelist.com › Home › Analysis › 29 Mar 2007*

[6] *Keyloggers* in Cyber security Education - Christopher Wood *Christopherwood.com/papers/KeyloggersInCybersecurityEducation.pdf*

[7] Priti Saxena, Bina Kotiyal, R.H.Goudar:A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India(April 18,2012)

[8] Mohammad Wazid,Robin Sharma, Avita Katal, R.H.Goudar, Priyanka Bhakuni :Implementation and Embellishment of Prevention of Keylogger Spyware Attacks(2013)

[9] Introduction to Cybercrime: Connolly, C. (2009) "Cyberlaw," *Hot Topics: Legal Issues In Plain Language*, No. 70, State Library of NSW. <http://www.legalanswers.sl.nsw.gov.au/hot_topics/pdf/cyberlaw_70.pdf>

[10] Insider Attack and Cyber Security, Beyond the Hacker(book) Salvatore J. Stolfo,Steven M. Bellovin,Shlomo Hershkop, Angelos D. Keromytis :*Columbia University, US.*

[11] http://www.b4usurf.org/index.php?page=software-piracy-and-the-law/

[12] http://www.crossdomainsolutions.com/feed/

[13] http://en.wikipedia.org/w/api.php/

[14] http://en.wikipedia.org/w/api.php/

[15] http://antikeyloggers.com/how-to-detect-keyloggers

[16] http://feeds.howstuffworks.com/DailyStuff

[17] http://www.onguardonline.gov/phishing

[18] http://howto.caspio.com/xmlrpc.php

[19] http://office.microsoft.com/favicon.ico

[20] http://www.microsoft.com/security/default.aspx