EXERCISE

Perform the following activity till you are confident:

S.No.	Activity
1.	Register with Junglee (www.junglee.com), Yatra (www.yatra.com) and practice online transactions.

ASSESSMENT

Answer the following:

1. Explain the purpose of Online transactions.
2. List any five websites that allow online transactions.
3. List any three payment tools to use online transactions.

SESSION 8: INTERNET SECURITY

Relevant Knowledge

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. This session introduces you to Internet security concepts and how to secure online and network transactions.

Though Internet provides valuable information and entertainment, it may leave your computer unsecure due to many online threats. You need to ensure that your usernames, passwords, credit card or online banking information secure as they are prone to be tracked and used by unauthorized users. Some websites can also install Malware on the computer without user consent thereby leaving the computer damaged or insecure.

Online threats such as Phishing, email spoofing, chat spoofing, etc. can increase the chances of users getting compromised.

You can reduce the risks by using best practices such as using Antivirus Software, Antispyware Software, Firewalls, strong passwords, etc. in addition to spreading awareness of the best practices.

Best Practices for Security

Use strong passwords, a combination of alphanumeric and special characters could be used for creating a password that is not so easy to crack or guessed by other users. Do not keep passwords such as your favorite color, friends or relatives name, bike number, mobile number either as single or combined option. These passwords are easy to guess if a user knows you personally. Change your password frequently at least 2 or 3 weeks so that your account information remains secure.

Using strong passwords can lower the risk of a security breach; effectiveness of a password depends on the security mechanism of the software and users involvement in generating a strong password.

Most websites check for password effectiveness when a user attempts to register for the first time or when they change password. For example, when you register with Gmail, you may notice a password meter displaying the strength of your password similar to the one displayed below.

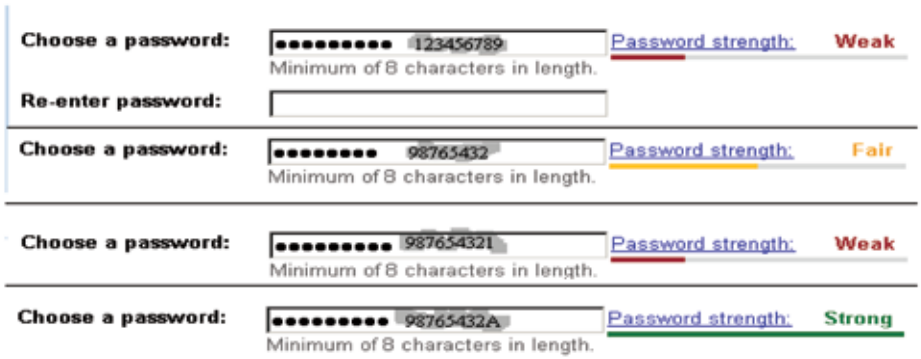

Figure 37

Following is a general guideline for managing strong passwords.

- Keep the length of the password at least 12-14 characters if permitted.
- Avoid keeping passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, etc.
- Including numbers, and symbols in passwords if allowed.
- Use capital and lower-case letters.
- Avoid using the same password for multiple sites or purposes.

- Avoid using something that the public or workmates know you strongly like or dislike.
- Use random password generators if possible.

Example of a strong password: **u1vX:,4Hd{]$**

You may also use websites such as www.strongpasswordgenerator.com that can generate random strong passwords. To generate a strong password using www.strongpasswordgenerator.com do the following:

- Open any web browser. Type www.strongpasswordgenerator.com in the address bar and press Enter.
- Click Generate strong password. Notice the password displayed under your new password.

Backup your data: Always keep copies of personal data in additional media such as compact discs, pen drives, etc. This could be helpful in situation when there is a loss of data. Keep the data away from unauthorized users.

Use encryption software: (Usually available within the operating system) to protect your data from unauthorized users. If encryption software is not available within the operating system, use a 3rd party software.

Keeping your username and password private: Never save your username or password on computers that are used in shared environments such as internet café. Browsers may save your personal data on the local computer that can be used by another user using the same computer.

Registering with websites: Read the privacy statement or policy whenever you register with a website, the statement or policy will include information about how the website use personal data.

Do not share personal information: Websites require you to fill out forms containing fields such as name, gender, age, email address, school, etc. Be cautious when filling out such forms; research and verify if it's a trustable website . Your email addressed could be used by unauthorized users to send you fake or unwanted emails; think twice or thrice before providing information to any website and decide if it is really necessary.

Secure transactions: If you are using online shopping or transactions, websites even store your credit card or online banking personal information such as your credit card number, account details, etc. This information can be tracked and used by un-authorized users often known as hackers to misuse this information. Again, ensure the website is legitimate and uses secure practices for performing and maintaining online transactions. Since information such as credit card details or personal information is sent over the network, it is always recommended to use only secure websites for such transactions. Verify if the website uses secure transaction; usually it is indicated through a digital certificate represented as a golden lock in the web browser's address bar.

Use antivirus and antispyware software: Computers are prone to attacks from software known as Malware that could harm your computer. Malware track browsing behavior or transmit personal data from your computer; programs such as keyloggers could be installed on your computer track and transmit every key that is pressed on a keyboard (keystrokes) to unauthorized users. Antivirus and Antispyware programs also offer real-time protection monitoring your computer for any changes by malware software. Keep your Antivirus and Antispyware software always up to date, this can help in protecting your computer from recent threats.

Do not immediately respond to mails from unknown users: It may be a fake mail trying to gather personal information such as your bank account details, home address, etc. Some mails could promise you jobs or announce lottery results which in turn could compromise the user. And in some cases, virus or scripts that are dangerous could be attached to the mail; NEVER open the attachment from an unknown source.

Clear browser cookies frequently: Cookies are programs that are created on your local computer when you visit websites. Though cookies are meant for storing data based on your activity performed during your earlier visit such as logon details, details of a shopping cart, visited pages in a website, etc. they could also be tracked by unauthorized users and possibly gain access to your personal information.

Keep the operating system and software applications up to date, though operating systems and applications are designed, tested and distributed, sometimes they may have security holes through which a hacker can take advantage; they may track and gather information or even damage the whole computer. In general, most vendors notify the users whenever a security hole is identified and an update is available to address that particular issue. You can also visit respective vendor's website to check if there are any updates available, download and keep your operating system and software applications up to date, free from security holes.

Install firewalls: Firewalls could be software or hardware and can assist in keeping a computer and a network secure. Firewalls analyze the network traffic and determine if the traffic should be allowed or not. In most cases, operating systems such as Linux, Windows or Mac include firewall software as a part of operating system thus keeping the computer secure. In rare cases, you may need to configure your firewall for additional security.

Never install software from unknown sources: As they might not be trustworthy; download only from well-known or reputed websites. Verify the source if it is legitimate by searching the internet or referring to comments from other users before downloading them; understand the nature and the purpose of the software before attempting to download and install them.

Remove unwanted or unknown software applications: These might have got installed without your knowledge when you have visited some websites. Unwanted software could get installed as they might have been bundled along with necessary software. Some programs such as toolbars get installed usually through bundled software and are programmed to send personal data without your consent.

Clearing Data Stored In Browsers

Web browsers have built-in password management designed to store passwords used in forms on websites. Browsers often prompt to save usernames and passwords when users attempt to logon to websites.

This facility is offered to users, so that they can logon to their frequently used websites without having to type the usernames or passwords. However it is not advisable to leave the web browser store this data particularly on public or shared computers.

To clear personal data from a web browser such as Mozilla Firefox, launch the browser.

- Click ***Tools*** Menu, click ***Options.***
- Click ***Security*** Tab. The following window will be displayed:

Figure 38

Notice that under ***Passwords*** section, ***Remember password for sites*** is checked. This means the browser is configured to save passwords for websites automatically. You can uncheck ***Remember password for sites*** option, if you prefer NOT to store passwords.

Mozilla Firefox can also store data such as cookies, visited websites or webpages data, browsing history, etc. To clear this stored data, click ***General*** tab > ***Option.*** The following window will be displayed:

Figure 39

- Click ***Privacy*** Tab. The following window will be displayed:

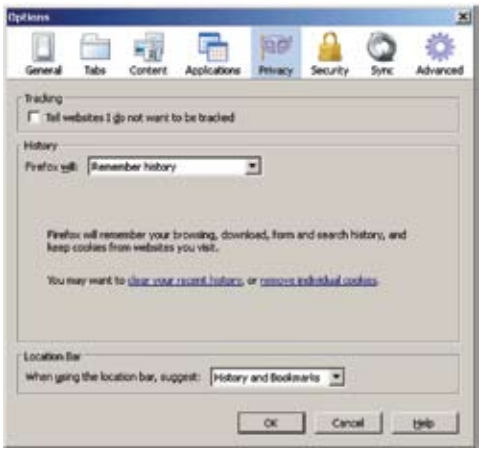

Figure 40

- Under ***History*** section, click the drop down menu next to ***Firefox will:.***

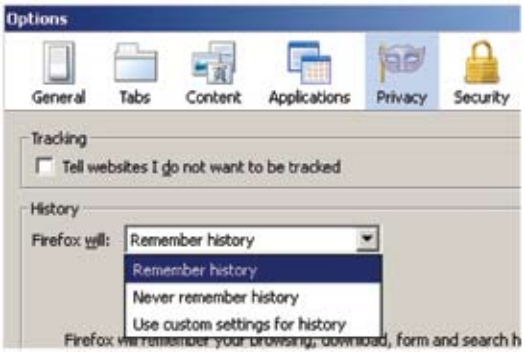

Figure 41

- Select ***Use custom settings for history*** from the drop down list. The following window will be displayed:

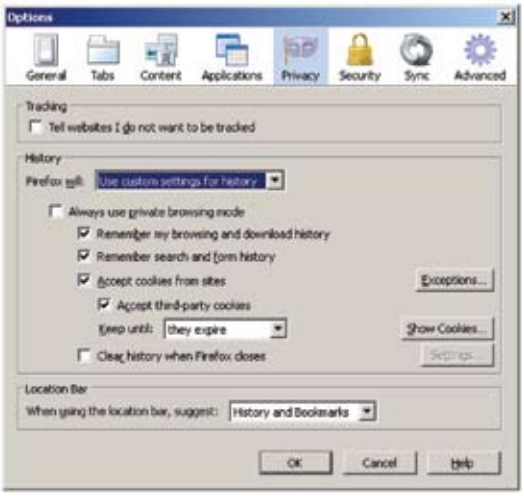

Figure 42

Notice the preferences; Firefox is configured to remember browsing and downloading history search and form history and cookies. If you do not wish store the above mentioned data, select **Never remember history** from the drop down list. If you are in a public environment such as a cyber café, you may select the option ***Clear all current history.*** On selecting this option, the following window will be displayed:

Figure 43

- Click ***Clear Now*** and then click ***OK.*** From now on, Mozilla Firefox will not remember any history as you have configured it that way.
- There are several online threats such as Phishing, email spoofing, chat spoofing, etc.
- You can reduce the risks by using best practices such as using Antivirus Software, Antispyware Software, Firewalls, strong passwords, etc. in addition to spreading awareness of the best practices.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	You have learnt to work with Mozilla Firefox. Now perform tasks outlined earlier using Mozilla Firefox with other browsers such as Internet Explorer, Google Chrome. Use the help file or online help to find procedures.

ASSESSMENT

Answer the following:

1. Explain the purpose of Internet Security.
2. Explain different kinds of online threats.