Identity theft is a fraud involving another person's identity for an illicit purpose. This occurs when a criminal uses someone else's identity for his/her own illegal purposes.

Examples – fraudulently obtaining credit , stealing money from the victim's bank account, using the victim's credit card number

How to prevent being victim of identity theft

Sr. No.	Security Measures	Brief of Description
1	Monitor your credit closely	The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you. Watch for suspicious signs such as accounts you did not open. You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security
2	Keep records of your financial data and transactions	Review your statements regularly for any activity or charges you did not make
3	Install security software	Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions
4	Use an updated Web browser	Use an updated web browser to make sure you're taking advantage of its current safety features
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages	Use caution even when the message appears to come from a safe sender as identity information in messages can easily be spoofed.
6	Store sensitive data securely	Just as you keep sensitive paper documents under lock and key, secure sensitive online information. This can be done through file encryption software
7	Shred documents	It is important to shred the documents that contain personal or financial information (both paper and electronic) before discarding them. This prevents dumpster diving and in the online world, the ability for hackers to bypass information that has not been permanently deleted from your system

8	Protect your PII	Be cautious about giving out your personally identifiable information (PII) to anyone. Find out why the information is needed and if it’s absolutely necessary to give out. Be careful about the details you provide about yourself online, such as on social networking sites.
9	Stay alert to the latest scams	Awareness and caution are effective methods to counter fraud. Create awareness among your friends and family members by sharing security tips you learn with them.

Spywares

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden from the user; it is secretly installed on the user’s personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate at public computer on purpose to secretly monitor other users.

It is clearly understood from the term Spyware that it secretly monitors the user. The features and functions of such Spyware are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users’ computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP).

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti- Spyware softwares are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practice perspective.

Malwares

Malware short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code. Malware can be classified as follows:

1. **Viruses and worms:** These are known as infectious malware. They spread from one computer system to another with a particular behaviour.
2. **Trojan Horses:** A Trojan Horse, Trojan for short, is a term used to describe malware that appears to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
3. **Rootkits:** Rootkits is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised.
4. **Backdoors:** Backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.

Virus and Worms

Computer virus ia program that can infect legitimate programs by modifying them to include a possibly evolved copy of itself. Viruses spread themselves, without the permission or knowledge of user, to potentially large number of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance. The combination of malicious code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g. triggered after a specific number of executions), time-driven effects (e.g. triggered on a specific date, such as Friday the 13th) or can occur at random.

Viruses can take some typical actions

1. Display a message to prompt an action which may set of the virus.
2. Delete file inside the system into which virus enter
3. Scramble data on a hard disk

4. Cause erratic screen behaviour
5. Halt the screen (PC)
6. Just replicate themselves to propagate further harm

A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention.

Backdoor

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.

A backdoor works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable. Most backdoors are automatic malicious programs that must be somehow installed to a computer. Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host. Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes. Attackers often discover these undocumented features and use them to intrude into the system.

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it get control and cause harm, for example ruining the file allocation table on the hard disk.

Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet. It is also possible inadvertently transfer malware through a USB flash drive or other portable media. It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines. (Users would not know that these could infect their network while bringing some music along with them to be downloaded.)

Unlike viruses or worms, Trojans do not replicate themselves, but they can be equally destructive. On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author: however it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. **Stay away from suspect websites/weblinks :** Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things.
2. **Surf on the Web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the Web.

   It may be experienced that, after downloading the file, it never works and here is a threat that – although the file has not worked, something must have happened to the system – the malicious software deploys its gizmos and the system is at serious health risk. Enabling Spam filter "ON" is a good practice but is not 100% fool proof, as spammers are constantly developing new ways to get through such filters.

3. **Install antivirus / Trojan remover software:** Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

Phishing

The word Phishing comes from the analogy that Internet scammers are using E-mail lures to fish for passwords and financial data from the sea of Internet users.

The E-mail will usually ask the user to provide valuable information about himself/herself or to "verify" information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:

1. **Names of legitimate organizations:** Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-mail.
2. **"From" a real employee:** Real name of an official, who actually works for the organization, will appear in the "from" line or the text of the message (or both). This way, if a user contacts the organisation to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.
3. **URLs that "look right":** The E-mail might contain a URL (i.e. weblink) which seems to be legitimate website wherein user can enter the information the phisher would like to steal. However, in reality the website will be a quickly cobbled copycat – a "spoofed" website that looks like the real thing, that is, legitimate website. In some cases, the link might lead to selected pages of a legitimate website – such as the real company's actual privacy policy or legal disclaimer.
4. **Urgent messages:** Creating a fear to trigger a response is very common in Phishing attacks – the E-mails warn that failure to respond will result in no longer having access to the account or E-mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

Examples of phrases used to entice the user to take the action.

1. **"Verify your account":** The organization will never ask the user to send passwords, login names, permanent account numbers (PANs) or SSNs and other personal information through E-mail. For example, if you receive an E-mail message from Microsoft asking you to update your credit card information, do not respond without any confirmation with Microsoft authorities – this is a perfect example of Phishing attack.
2. **"You have won the lottery":** The lottery scam is a common Phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often

includes references to big companies, for example, Microsoft. There is no Microsoft lottery. It is observed that most of the phished E-mails display the name of the agencies/companies situated in Great Britain and hence it is extremely important for netizens to confirm/verify the authenticity of such E-mail before sending any response.

3. **"If you don't respond within 48 hours, your account will be closed":** These messages convey a sense of urgency so that you will respond immediately without thinking. A Phishing E-mail message might even claim that your response is required because your account might have been compromised.

Phishing vis-a-vis Spoofing

1. Phishing is used to get the victim to reveal valuable (or at times invaluable) information about him/her. Phishers would use Spoofing to create a fake E-mail.
2. Spoofing is not intended to steal information but to actually make the victim do something for phishers.
3. Phishing may, at times, require Spoofing to entice the victim into revealing the information but Spoofing does not always necessarily result in Phishing someone else's account.

The Combined Attack – Phishing and Spoofing

Phisher sends an E-mail, during Income Tax return filing period, from an official looking IT (Income Tax) account which is spoofed. The E-mail would contain URL to download a new tax form that was recently issued. Once the victim clicks the URL, a "virus cum Trojan Horse" is downloaded to the victim's system. The IT Form may seem official, but like a Trojan Horse, the payload has already been delivered. The virus lies in wait, logging the actions of the victim. Once the victim inputs certain keywords, like bank names, credit card names, social networking websites and so forth, it logs the site and the passwords used. Those results are flagged and sent to the phisher. The virus could then gather the user's E-mail contacts and send a fake E-mail to them as well, containing the virus. The phisher now has gained the required personal information as well as virus was sent, downloaded, and spread to entice other netizens.

How to avoid being victim of Phishing attack

Sr. No.	Security Measures	Brief of Description
1	Keep antivirus up to date	Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
2	Do not click on hyperlinks in E-mails	It should always be practiced that, in case an E-mail has been received from unknown source, clicking on any hyperlinks displayed in an E-mail should be avoided. This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check out the link, manually retyping it into a web browser is highly recommended.
3	Take advantage of antispam software	Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-spam software, many types of phishing attacks are reduced because the messages will never end up in the mailboxes of end-users
4	Verify https (SSL)	Ensure the address for displays " https://" rather than past "http://" along with a secure lock icon that has been displayed at the bottom right hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double clicking the lock to guarantee the third-party SSL

		certificate that provides the https service. Always ensure that the webpage is truly encrypted
5	Use anti-Spyware software	Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti- Spyware software can often detect the problem and provide a fix
6	Get educated	Always update the knowledge to know new tools and techniques used by phishers to entice the netizens and to understand how to prevent these types of attacks. Report any suspicious activity observed to nearest cyber security cell
7	Use the Microsoft Baseline Security Analyzer (MBSA)	The netizens on the Microsoft platform should use MBSA to ensure the system is up to date by applying all the security patches. MBSA is a free tool available on Microsoft's website. This protects the IT systems against known exploits in Internet Explorer and Outlook and Outlook that can be used in Phishing attacks
8	Firewall	Firewall can prevent Malicious Code from entering into the system and hijacking the browser. Hence, a desktop (software) such as Microsoft's built-in software firewall in Windows-XP and/or network (hardware) firewall should be used. It should be up to date in case any cyber security patches have been released by the vendor
9	Use backup system images	Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play;
10	Do not enter sensitive or financial information into pop-up windows	A common Phishing technique is to launch a bogus pop-up window when someone clicks on a link in a Phishing E-mail message. This window may even be positioned directly over a legitimate window a

		netizen trusts Even if the pop-up window looks official or claims to be secure entering sensitive information should be avoided because there is no way to check the security certificate
11	Secure the hosts file	The attacker can compromise the hosts file on desktop system and send a netizen to a fraudulent site. Configuring the host file to read only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe
12	Protect against DNS Pharming attacks	This is a new type of Phishing attack that does not Spam you with E-mails but poisons your local DNS server to redirect your web request to a different website that looks similar to a company website (e.g. eBay or PayPal).