Asian Social Science; Vol. 13, No. 12; 2017
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Understanding and Protecting Yourself against Threats in the Internet

Ajith Sundaram[1,2]

[1] Research Scholar, Anna University. Chennai, India

[2] Assistant Professor, Rajagiri Centre for Business Studies, India

Correspondence: Ajith Sundaram. E-mail: ajithsundaram@gmail.com

Received: August 8, 2017 Accepted: October 2, 2017 Online Published: November 28, 2017

doi:10.5539/ass.v13n12p201 URL: https://doi.org/10.5539/ass.v13n12p201

Abstract

Reporting the incidents related to Computer Security has now become one of the most important component of the Information Technology programs with the increase in the attacks related to cyber security. The reason being the introduction of new and new security related incidents every day. It is giving light to the necessity of a quick and efficient incident response capability which could detect incidents, minimise the loss due to the destruction and mitigate the weaknesses that was exploited. This publication is a parameter for incident handling, especially for analysing event-related data and defining the appropriate response to each incident.

1. Banking Securely Online

1.1 Introduction

Online banking, ever since its inception, has posed threats to financial and personal security. Many users had been a prey to online banking threats. In order to avoid getting caught in the trap, one should get accustomed to various frauds and risks and secure by taking adequate precautions to avoid getting into security-related troubles. The following actions, to a greater extent help in avoiding security-related online banking problems:

- Assess and evaluate privacy and policy details
- Use complicated login details
- Secure your computer
- Have a check of available account balance periodically
- Refrain from accessing accounts from public places
- Enhance Credit cards usage
- Check email communications from banks regularly
- Ensure swift action when account is intruded into

1.2 Online banking attacks

A few of the widespread types of online attacks are

1.3 Phishing attacks

Phishing attacks are planned by using counterfeit emails or messages from an agency or person posing as a representative of the bank. The mail/message requests for personal, sensitive, banking data which needs to be typed into a link connected to a fake website. Once the link is followed and sensitive details are disclosed, intruders can gain access to banking related data. Phishing attacks also arise from pop-up windows with the real website address. Any data typed will reach fraudulent users. In a similar fashion, vishing is a fraud method where a person calls and pose as a bank authority to seek account details.

1.4 Malware

Malware is a software code initiated with evil purpose. Such malicious computer programs enable the user into trusting traditional security system for protecting during online transactions. Such softwares are designed to perform some of the following operations

- Steal account related data- malware monitors and captures login data including all the special characters, words or images used
- Fake website substitution- capable of generated illegitimate web pages that looks real. Such site enables an intruder to intercept user data without the knowledge of the user
- Account hijacking- malware hijacks the browser and transfer data and funds without the user's knowledge. Whenever logged into bank website, the software creates a hidden browser that reads account balance and enable fraudulent fund transfer to the intruder's account.

1.5 Pharming

This involves installing a secret and dangerous code on the computer that enters through an email or an attachment. Later, the user goes into a fake site that closely looks like the bank website. Any data entered is acquired by the intruders.

One interesting feature to be considered is that all the above attacks use technological acumen, which again is got only from the callous attitude of the user in his/her online money management. Though there is absolutely no assurance of safety related to online banking certain good practices can inhibit the fraudsters from attacking accounts.

Periodic review of bank's online privacy features and actions- banks should mandatorily send a copy of the privacy features to all their customers. Customers, from their side, are required to ensure that they adhere to additional security features authorised by the bank.

Check the privacy policy of the company before initiating online payments- always refrain or limit from disclosing unwanted private data. Also view any existing history of privacy violations from the bank's side.

Always choose a complicated online personal identification number (PIN)- always update or change PIN regularly. Avoid easy to guess numbers like birthdays. Never disclose PIN number to others.

Install powerful anti-virus or anti-spyware programs and update them frequently- always keep an updated version of anti-virus installed the computer to avoid gaining illegitimate access. Periodically agree to system upgrades.

1.6 Regular assessment of online account activity

Using credit card for online payments- credit cards have powerful protection than debit cards

Refrain from accessing accounts in public places where chances of public monitoring are high- avoid entering log in details from unsecured or public networks. Avoid computers or systems that are easily accessible by public as sometimes the account details can be deposited in the web browser's provisional memory.

Always verify emails relating to online banking and check the authenticity of the contents and the sender- avoid clicking suspicious links or replying to email requests or warnings regarding financial activity. As a precaution, forward the suspicious mail to the concerned authority and delete them from mail box.

Any disclosure made by the user on a fraudulent website regarding financial activity must be immediately reported

Agreed that online banking has its own risks. However judicious management of online activity will go a long way in preventing unauthorised access of financial information. Accustom to the rights and responsibilities of an online banking customer.

2. Cyber Threats to Mobile Phones

2.1 Increasing mobile threats

Smartphones or mobile phones, equipped with advanced features and capabilities as found in personal computers, are a hit with people. Despite its popularity, smart phones have become gullible objects for attackers. Though smartphones have outnumbered PCs in terms of units sold, they have become easy targets for attackers who have completely exploited their growing popularity. The attackers have resorted to sophisticated attacks on mobile phones which are more vulnerable than PCS, as they are yet to be equipped with counter attack measures. Smart phones and personal digital assistants provide users with facilities like internet and many other applications. Mobile phones are yet to embrace sophisticated technical security measures and use obsolete mobile phone operating systems. Mobile social networking do not own detailed privacy controls unlike the PCs. Sadly, most of the smart phone users are unaware of the security shortcomings. They remain ignorant of the fact that surfing internet on the mobile phones are as unsafe as surfing on PCs and that security softwares require to be enabled. Most of the users store sensitive data which are easy targets for attackers.

Mobile phones have become sophisticated and multiple utility devices with people using them to store emails, passwords, banking details, online transaction activities. They are easy prey for attacks due to their portability features as they are easy to rob and stolen phone exposes all the details to a shrewd attacker. Most of the apps are malicious as anyone can design apps for mobile operating systems with scant regard for safety. Sources that are not linked to mobile service providers offer unfettered apps that can break into locked phones by bypassing the lockout features. Just like in PCs, legitimate smartphone softwares can be attacked. The user himself can trigger off an attack clicking on a link that gives rise to passive attack or by just using a handset that has a susceptible app.

Phishing attacks use electronic communications to trap users into installing dangerous softwares. Just like in PCs, mobile phone users are susceptible to phishing, smishing and vishing attacks on both feature phones and smartphones. Users may receive fraudulent charges on their mobile phone bills or by soliciting donations especially in the name of donations after any major catastrophe. Mobile phone users consider the phone's security to be less important whereas in reality it can be controlled by an attacker by enabling it to perform harmful commands. Smart phones are also great carrier of viruses.

2.2 Steps to protect mobile phone

Mobile phones have also developed sophisticated security solutions which were previously available only for PCs. Moreover, the security of the mobile phone is vested with the user who has to be cautious and judicious in matters relating to mobile security. In spite of taking precautionary measures, users can fall prey to mobile phone attacks. However, by adopting mobile phone security measures, the likelihood of an attack can be prevented.

- **Choose phones that give emphasis on security features-**Choose a device that offers file encryption that deletes malicious apps, that enable the service provider to erase the device remotely, that has an option to encrypt a backup, if any or that which support certificate based authentication.
- **Secure the device through configuration-** use password feature available in smartphones. By enabling this feature, by choosing a complex password, enabling encryption, remote wipe abilities and antivirus application all go a long way in protecting the mobile phone.
- **Configure web accounts to enable secure connections-** enabling configured web accounts prevents attackers from accessing web sessions
- **Refrain from accessing suspicious links or emails or messages-** they can lead to malicious content
- **Refrain from posting mobile number in public websites-** attackers can access mobile numbers from public websites and use them for future attacks

- **Choose what to store in the device-** be wise in storing data in the device as attackers can have access to the stored content with enough time and sophistication
- **Choose apps wisely-** research on apps before installing them. Check on what details the app solicits. Do not install the app if it demands too much permissions for installing. It can turn out to be Trojan horse
- **Have control of the device in public places**- the portability of mobile phones make them easy to be stolen. So have a physical control of the gadget
- **Disable interfaces that are not in use-** attackers look at loopholes in the softwares that use the interfaces
- **Keep Bluetooth enabled phones to non-discoverable mode-** keep the Bluetooth enabled in non-identifiable mode to make it invisible to fraudulent devices. If Bluetooth enabled devices are in discoverable mode, they can attract an infected device or attacker as they expose their visibility to them
- **Avoid using unknown wi-fi networks or public wi-fi-** attackers may identify vulnerable devices from public wi-fi networks and can attack mobile hotspots
- **Delete all data before disposing a device-** contact the device's manufacturer to understand about how to securely wipe the device before discarding
- **Be vigilant when using social networking applications-** the apps reveal unwanted personal details and location to unintended parties
- **Do not intrude the device-** third party firmware should not be used to access the device features that are locked by default.

Timely action when smartphone or personal devices are stolen/lost

- **Report the loss of the gadget to the organisation and mobile service provider-** intimate the loss to the organisation and service provider as soon as possible to hinder the malicious activities
- **Convey the authorities/police about the loss-** appropriate actions can be taken by the local authorities when theft of gadgets are reported
- **Change account permits-** when phones are used to access corporate networks, contact the IT faculty and revoke all the stored content on the lost phone
- **If required, wipe phone-** if possible erase all the stored data on the phone by contacting the service provider

3. Play Safe: Avoid Online Gaming Threats

Sophisticated machineries, skills and high speed internet led to the rising popularity of online gaming. This has enabled pranksters and fraudsters to venture into this arena for illicit profits. Anybody using online games must be educated about the risks involved. Some of them are

- Interactions with cunning strangers who trick people into disclosing sensitive information
- Computer intruders who make use of security limitations
- Online and real world predators
- Viruses, compute wares and spyware

Some of the popular genre of games involve players to create online identities which perpetuate into real world activities. Virtual games are sold in real world for money. Similarly, real money is used to buy virtual world games. This activity has given rise to virtual crime. Online games are prone to technological risks and social risks.

3.1 Technological risks

a) **Viruses and worms-** they come in the form of attachments in mails, messages or through game files or installed softwares and intrude the computer systems

b) **Malicious software-** fraudsters also capitalise on social networks linked to online games and solicit the users to fake websites or to open email attachments carrying dangerous software or content.

c) **Insecure or compromised gamer servers-** insecure software on the game server poses a risk to the computer on which it is connected. Any game working using internet or connected to another computer is risky compared to the ones that is not linked to internet. Attackers can choose to install spyware, viruses or access personal details from vulnerable systems. By exploiting vulnerable codes available in online games, pranksters can read files, crash games and have complete control of the computer. Similarly operating a computer server running gaming apps involve the same risks as those involved with the operation of servers of other applications. Attackers can crash the server if it has poor security profile or insufficient protection. Sometimes, gaming protocols are inefficiently implemented and are not secure as other popular commercial softwares. As a result, it exposes the computer to unknown attacks.

3.2 Social risks

Computer games, which were once solitary activities, have expanded to online communities. Intruders have harvested these interactions in such gaming environments to gain access to personal or sensitive information. Some of the social risks associated with online gaming are

a) Social engineering- attackers may lure into installing softwares that can control and monitor online activities and lead to fake websites that offer malicious downloads on the pretext of online game apps

b) Identity theft-fraudsters can gain personal data from the gaming profile and can create fake profiles or accounts in the stolen name or can even use it to access financial accounts.

c) Protection schemes- there has been a rampant crime happening in gaming community. Protection rackets operate by warning weaker players of the community of negative consequences if real money is not paid.

d) Cyber prostitution- sometimes pranksters create fake cyber brothel soliciting customers. And once the money is paid, the account gets deleted

e) Virtual mugging-the players used software applications to defeat other players and took away their items to be sold online.

f) **Virtual sweatshop-** exchange of simulated items and virtual currency for tangible money has produced cybernetic sweatshop where workers from poorer countries are abused by people seeking profits from online economies

3.3 Protection from risks

By educating oneself about computer security, internet gaming can be safe and enjoyable. Basic computer security principles that need to be followed are using antivirus, using firewall, checking the authenticity of the downloaded files, cautious in opening attachments, creating a backup of financial data, using complex passwords and updating application software.

3.4 Gaming-oriented security principles

a) **Identifying 'administrator mode' risks-** some games demand using the computer in admin mode. In such cases, it is imperative to ensure that the game vendor is authentic and reliable and the game has to be downloaded only from a trust worthy site. Free downloaded games are embedded with malicious software involving plugins that require that require to run certain games. In admin mode, the attacker can have a complete and easy access to the computer. And always ensure that the administrator password is private and close monitoring of kids' online activities are advised.

b) **Identify ActiveX and Javascript risks-** always be aware that some web games require ActiveX or Javascript to be enabled. This exposes many risks when the features are enabled.

c) **Play the game on the game site-** it is always advisable and safe to play online games at the game site itself. This way, one can switch back to the user account to browse the web. This reduces the risk of landing on to a malicious website.

d) **Pay attention to firewall management-** home users can use firewalls to safeguard their computers from risks. When multi player internet games are player, certain rules prompt the firewall to be lax inorder to gain access to the computer. In such settings, there are higher chances of security threat to the computer. Sometimes, firewalls may allow certain IP addresses to be tagged trusted to reduce the chance of interacting with a fraudster who can infect the computer.

Online games are a great source of entertainment generating new industries and revenues and opening up the imagination of individuals. However, there are also risks involved, which can be dealt through judicious security management techniques.

4. Introduction to Information Security

As per the reports of Internet Software Consortium's Internet Domain Survey, as on January 2008, approximately 542 million computers available over 250 countries on every continent, including Antarctica, was connected to the internet. The internet can be described as worldwide assembly of lightly linked networks, which can be reachable by distinct computer hosts, in many different ways, to any person owning a personal computer and an internet connection. The internet is not a single network and can be reached by individuals and organisations, irrespective of the national or geographical frontiers at any time of the day.

However, the ease and stress-free accessibility to data is laced with security threats and risks, the foremost risk being loss, theft or misuse of information. The data stored electronically and made available on networked computers are more susceptible to risks than those printed on paper and stored in cabinets. Intruders need not be physical present to steal data. In fact, they may operate from beyond geographical boundaries. They can steal or fiddle with the electronic content without leaving any trace of their illegal activity. They can generate new electronic documents, work on their own programs and keep their unauthorised activity under wraps.

4.1 Preliminary security theories

The preliminary security theories relating to content on the internet are confidentiality, availability and integrity. Security models relating to individuals who access the content are authentication, authorisation and nonrepudiation. When data is accessed by an unauthorised person, the result is loss of confidentiality. Confidentiality is pivotal to information like research data, health and insurance documents, new item dimensions and corporate venture strategies. There is a legal compulsion to defend the secrecy of individuals or organisations, principally for banks, loan firms, debt collectors, companies offering credit facility, hospitals, medical practitioners, medical records, institutes offering counselling or rehabilitation, tax collecting agencies. Information when available on an insecure network gets infected and the content gets modified. This result is called loss of integrity. Human activity by way of error or tampering can cause unauthorised changes to the content. Integrity is crucial for safety particularly for financial accomplishments such as electronic fund allocations, air traffic mechanism and financial accounting. When data becomes unavailable due to inaccessibility or if deleted, the result is loss of availability. This means that the required content cannot be accessed by authorised individuals. Availability feature is the most important element in service related businesses which predominantly use the information.

Availability of the network is imperative to businesses that are dependent on network connection. When users are denied or are unable to access the network or those facilities offered on a network, they go through denial of service. Authentication and authorisation are used by organisations in order to make the information available to those who actually require it. Authentication is establishing that the user is actually the same person who he/she claims to be. To prove the point, the user may have something tangible such as a smartcard or some hidden code like a password or something that proves the user's identity like fingerprint. Authorisation involves finding out if the person/system has the power or right to operate certain activity on the system. Authentication and authorization operate simultaneously. Users should authenticate themselves before undertaking the operation they are authorised to carry out. Once authentication is done, the user cannot deny his/her action. Security is strong in such cases. This inability to deny the act done is called nonrepudiation.

Internet users always need to be assured of information security. That is, they should be convinced that

- The information they use is trust worthy
- The data for which they are responsible will be used only in the manner that is expected to be shared
- The information will be available for use when required
- The systems will process content in timely and trustworthy mode.

Information security assurance goes beyond system of different kinds like large scale systems, regulation systems, in-built system and it accommodates systems with hardware, software and mortal elements. It also takes care of system intrusions and laxity towards information safety.

Strangely, it is easy to get into an insecure network and gain unauthorised access to data. And above all, it is difficult to nab the intruders. Though, nothing worth stealing is stored on the system, intruders can use the computer as a weak link, paving way for unauthorised access to organisation's systems and information.

Sometimes those data that are normally considered unimportant or harmless, like type of hardware or software used, system patterns, type of network connections, contact numbers, access and authentication actions are of great interest to intruders. System security is at risk when security oriented content enable intruders to connect to important files and programs. Examples of important content are passwords, access control files and keys, manpower details and encryption processes.

All are vulnerable to security lapses and intrusions. Those affected comprise banks and financial institutions, insurance organisations, brokerage houses, consultants, government organisations, medical centres, medical laboratories, network service providers, functional institutions, education services, wholesale and retail traders. Some of the aftermaths of an intrusion are major loss of time in recovering from unruly situation, downward productivity, huge loss of money and man-hours, significant loss of credibility or business opportunity, legal liability, business crash and even loss of life. Sometimes, individuals may even go bankrupt due to leak of valuable information like financial content. Individuals can lose valuable details like credit card PIN, medical and other personal and confidential information. Individuals must be abreast with websites data that include alerts, cyber security tips, authorised people related to information security systems and people in power who may be capable of taking control of the situation and initiate appropriate action.

5. Understanding and Protecting Yourself Against Money Mule Schemes

Money Mules Are those people who are used to commit fraud by transporting stolen money or some kind of goods. Fraudsters recruit money mules to grab stolen credit card details. Sometimes, money mules are unaware of the fact that they are being used to commit fraud. But there are also money mules who participate willingly. The modus operandi is to extract money from organizations or from individuals.

5.1 Schemes that look like legal options

The rampantly used money mule efforts are in the form of 'work from home' solicitations. They focus on the unsuspecting people who may be desperately looking to work from the comforts of their home. The solicitations are meticulously crafted so as to look like genuine offers from legitimate companies. Fraudsters structure the content or mail in such a manner that they are not filtered by spam filters and is designed to appear like communication from recognised companies. They even go to the extent of posting on jobsites where job aspirants are caught unawares.

The money mule scheme goes on like this:

Once the individual exhibits interest, the fake company gathers information like bank details and social security number from the employee, that is, the victim. He is also asked to sign a document that resembles a contract. As per the instructions from the company, the employee creates a financial account for funds transfer. The employee receives funds which are directed to be sent to a third party criminal. Many money mules operate this way and once the stolen fund is received by the criminal, the relationship is dissolved. The criminal recruits another mule for the next fund transfer. Throughout the process, the criminal's identity, involvement and intentions are hidden.

5.2 Consequences

The criminal and the other parties involved in the scheme will face serious consequences if caught and found guilty. The potential penalties are

- **Inaccessible bank accounts-** the law enforcement authorities may freeze the mule's bank account which may result in financial crisis. There will be a burden due to the long term impact on credit sources
- **Prosecution-** money mules will be taken for a trial for their involvement in fraud.

  Responsibility for the damages- some mules found guilty will be held accountable and may have to repay the losses suffered by the victims.
- **Threat to personal data**- fraudsters are most interested in the personal information. They collect them from the money mules and can use them for malicious purposes.

Effect on individuals- The individuals who become victims may undergo the following consequences:

- **Financial loss**- an individual may lose money by paying for undelivered goods or money may be debited from their accounts. Depending on the charges framed or if culprits are booked, the individual may recover a part of the money lost.
- **Time consuming processes**- many hassles are involved right from identifying and reporting fraud to money recovery

Effect on organisations- when organisations are targeted, both the organisation and customers are affected.

- **Financial loss-** a fraudster may swindle a great deal of money.
- **Loss of sensitive data-** the criminal can steal customer data like financial data or use money mules to abuse customers
- **Goodwill loss-** the trust and loyalty of the customers will be lost if the organizations falls into fraud trap
- **Complicated processes-** many hassles are involved right from identifying and reporting fraud to money recovery
- **Possible future threats-** when prompt reactive and proactive measures are not taken, the organisation may fall into a new trap in future due to the loss of sensitive codes.

5.3 Steps to protect self

- **Do not fall into money mule trap-** look out for warning signs and double check before volunteering to participate. On suspicious activity, immediately report to the concerned authorities

- **Warning signs-** the job offers that are fake do not describe the job duties, company location will not be disclosed, the candidate specifications may not be highlighted, only online interaction take place and above all lucrative offers are made for little efforts. The most important warning sign to look out for is the email address as it uses a web-based service rather than the company domain.
- **Research-** do a thorough research about the company, the contact person and the offer. If no significant result arise out of the research, be convinced that it is a scam and report to appropriate authorities.

5.4 Steps to protect organisation

Criminals use fraudulent methods to connect to organisation's network and gain administrative access by using malicious code. By following certain preventive measures, organisation can reduce risks.

- Use strong firewalls, antivirus and anti-spyware software
- Restrict sensitive data to authorised staff only
- Always have a check on official records including employee data and financial transactions. Identify loopholes in the HR list
- Isolate computers used for performing banking operations. Apply strict access controls to such computers
- Look out for suspicious employee behaviour

6. The Perils of Using Portable Devices

Portable gadgets like jump drives, pen drives, personal audio devices and tablets offer users appropriate right to use corporate and personal data as and when needed. The increase in their uses is coupled with the increase in risks and threats. The fact that these devices are portable and enable them to connect to various networks and hosts make them prone to security breaches. These portable devices are vulnerable to theft which result in huge data loss, prone to data exposure when the confidential data is exposed to unauthorised people and susceptible to exposure to network oriented attacks to the system to which the device is connected.

6.1 Describing Portable Devices

There are two subsections of portable devices:

- Basic media devices that use a wired connection to a host transferring data (example, jump drives, mass media cards, CDs, DVDs and music devices without Wi-Fi competency)
- Smart media devices that can move data with a wired or non-cellular wireless association (for example, tablets, gaming devices, music devices with Wi-Fi competency and e -readers). These devices are predominantly used to check email, browse web and download various applications, audio and files

6.2 Risks involved

Using simple storage media looks safe, but it poses many hitches for a user or an organization. Most of the malware (malicious content) is transferred today through USB tools. These tools such as a jump drive or music device plug into the USB port of the PC and can enclose malware that is copied unintentionally or may get attached automatically. Attackers have become tech-savvy and have designed sophisticated methods to launch malicious code. Once a system gets affected, the malware spreads to other system in the network. These devices are capable of installing malware inside any firewall set up on PC and are not easily detectable. The portable storage devices being handy, gives easy access even for insiders to indulge in malpractices as they are hard to track.

Smart gadgets stealthily infect systems when downloading some content that has virus. Their rampant usage by a huge population and the absence of effective security tools make them great carriers of malware. There is also a large scale loss of data or data exposure as people tend to store sensitive content in their smart devices which when run on untrusted applications pose risk. Also, the attractive features of some of the smart devices attract threats. For instance, when Bluetooth is on, the device becomes visible to malicious attackers. Similarly, private and public wi-fi networks are hotbeds for attackers to intercept unencrypted data. The most common threat to smart devices is the handiness of the device. It can be easily left behind and is easy to be stolen.

6.3 How to Minimize These Risks

Some of the recommended practices to reduce the risks are

1. **For portable storage media - when making use of storage media such as jump drives, CDs and music devices without Wi-Fi competency**

- Install antivirus software powerful enough to detect any malicious attacks after scanning
- Refrain from connecting any unknown jump drive or media device to PC before checking it from IT personnel
- Disable aurorun and autoplay features from all portable media devices
- Ensure that there are separate devices for storing professional and personal data and run it only in the allowed systems.
- Secure all confidential content using powerful encryptions. Once the data is copied or transferred from a USB drive, ensure that it is deleted using delete utility

2. **For portable smart device when using smart tools such as tablets, music devices with Wi-Fi competency and e-readers:**

- Protect the tool by means of a strong PIN or secret code or password and alter it frequently.
- Download content only from trusted, verified and reliable sources or from the commercial store recommended by the device manufacturer

- Scan the entire device periodically by running anti malware software and take appropriate action when suspicious applications are detected
- Set an idle time out for the device to lock, in case there occurs a time delay in using it.
- If the device support location tracking, activate it to track the location of the device if it gets lost or stolen.
- Disable Bluetooth or wifi when not using it.
- Do not attempt to jail break the device, that is, do not try to remove the limitations set by the manufacturer
- Activate a remote-wiping facility to delete all contents on the device when misplaced
- When using wi-fi, ensure that the network is encrypted

3. For portable smart devices that are used in organisations

- Educate the employees about the policies imposed on the use of the kinds of removable devices allowed into the work environment. Ensure that the device has a significance in a particular business case
- Create acceptable policies for all removable devices used by the employees
- Advise the employees to report any missing devices inorder to wipe out data
- Advise the employees to use strong, secret codes for the devices
- Access should be allowed only through a protected VPN connection
- Ban personal portable devices in work set up
- Organisation may consider the feasibility of distributing corporate controlled devices for the employees
- Have a check list of mobile storage devices that carry important data and audit them on a regular basis.

7. Socializing Securely- Using Social Networking Services

Social networking enable people to receive and disseminate data with others online. People all over the world communicate with each other from their mobile devices, applications and websites. Reports prove that Facebook is accessed by more than 500 million active users, Twitter by 175 million users, MySpace by100 million and LinkenIn by 80 million. These social networking sites provide different purposes, the primary one being networking with others. Apart from that they are used for building new associates, reconnecting with old friends, maintain existing relationships, promote professional assignments or discussions. Sites like Facebook and Twitter cater to wide range of people whereas LinkenIn stands for professional networking and interactions. MySpace caters to those interested in music and entertainment.

7.1 Risks Involved

One should be cautious and have awareness regarding the likely hazards of sharing information on networking sites.

- **Threats and over disclosure of information**

  Pranksters may attack social media services and spread malwares, access personal information like identity, location, relationship details, etc. Sometimes, the users themselves may reveal too much information than intended to unauthorised individuals.

  1. **Viruses-** social networking sites are an ideal breeding ground for viruses given their immense popularity. When a virus is created and embedded in a website, the attacker puts many unsuspecting users to risk who transfer the malicious links with their list of friends.
  2. **Tools-** fraudsters make use of tools to regulate a user’s account and then accesses the personal information of the users and the contacts he share. There may also be an attacker posing as an imposter.
  3. **Social engineering attacks**- the attackers may post a comment or content that looks to be initiated from a genuine networking service. If acted based on the instructions, the user may end up revealing too much information or pave way for computer attack.
  4. **Identity theft**- when personal information lands into the hands of the attackers, they may assume the identity of the user and post contents in his/her name
  5. **Third party applications-** sometimes social networking sites allow addition of third party applications. Though it may look harmless, it is capable of accessing intimate details without the knowledge of the user and post content, send spams, access friends list, etc.

- **Professional and personal effects-**professional or persona relationships may be compromised due to unscrupulous access

  1. **Business details-** disclosing official content on social sites are unethical as well as harmful and causes considerable damage to professional life. Revealing customer details, internal issues of the company, intellectual property or other company matters on social media may bring about a bad reputation.
  2. **Professional status-** inappropriate photos or posts on social networking sites may destroy the professional prospects. Recruiters or colleges may verify the accounts of their prospective candidates during the screening process. Contents posted by the candidate that reveal the political, religious or social orientation may hinder the chances of selection and affect the credibility or reliability of the candidates. There have been incidents of people being sacked from their jobs for the kind of contents posted.
  3. **Personal relationship-** it is difficult to control the audience for certain posts. The comments, photos or contents posted impulsively may do much harm to personal relationships. Being transparent about the personal life on social media does much damage than expected as it is difficult to retract immediately. Almost 33 percent of the users have expressed their regret for revealing too much information.

4. **Personal safety-** there have been many incidents of cyber bullying. The contents posted may harm not only the user but also many others who are tagged in the posts or photos. The information posted unsuspectingly may invite unwanted harassment. Posting details such as the location, address, children's school details are much dangerous and may even compromise on the child's security. Cyberbullying incidents have harmed many individuals psychologically. So, social media pose as a physical, psychological or even social threat to the user if he does not manage his account meticulously.

7.2 Treading with Caution

The user must always be aware that the social media is filled with risks and security threats. With adequate proactive measures, this situation can be altered into an enjoyable process. Proper security measures adopting will protect the user as well as the computer from malicious attacks. By protecting oneself, those connected around can also be secured.

7.3 Putting security measures into use

Social media offer unique risks. However, the user need not panic when using social media. The risks can be minimized and can be made entertaining and informative by adopting certain precautionary and proactive measures. The following points need to be remembered while using social media.

- Set strong, complicated and difficult to guess passwords for each service.
- Always keep the anti-virus softwares updated
- Timely installation and updating of applications and softwares are pivotal to system safety
- **Use strong privacy settings-** the security options provided by the social networking sites should be completely implemented into the account. By taking advantage of the services provided, the user is protecting self, others and the computer system. Do not compromise on the security and choose appropriate action for better protection of privacy. The services may update their security settings periodically. So always keep a tab on the safety features provided and regularly evaluate the settings and options, looking for changes and choosing the safest feature. A regular review of services' privacy policies are recommended to ensure that the user has adopted and incorporate all the necessary measures..
- **Do not encourage suspicious third party applications-** choose third party application judiciously. Do not install suspicious looking softwares or those devised by unscrupulous or unreliable vendors. Keep a check on the amount of details that third party applications can access. Always look for applications developed by trust worthy vendors.
- **Remember that everything is public-** be aware that anything posted on social media cannot evade public access. So the intelligent way to protect oneself is by limiting the amount of personal data posted on social media. This applies not only to the profile of the user, but also is applicable on the contents, comments or images posted. Always be vigilant about the responses from fellow users. Be cautious on the kinds of contents posted about self, others and particularly children. Always refrain from divulging details about children as it may attract criminals to the children which may cause irreparable harm to them.
- **Share information only with known people-** social media provided the option of choosing an audience for posts. While posting content choose the right viewers who can see the posts. Though many users try to increase their contact lists, consider sharing contents with the appropriate audience. Always group the contacts and assign access features differently for each group. Attackers are shrewd enough to convince users to include them in their close circle. They may even adopt fake identities to convince the user to be added as a contact. Double check the authenticity of the new contact b and confirm the identity who they claim to be before letting him access the personal details. However, it is recommended to always add people known to the user than add unknown fraudsters just for the sake of expanding the contacts base. Better be cautious than regret later.

Regardless of extreme restrictive and privacy measures adopted, social media are not competent enough to provide complete privacy. It is these loopholes that attackers will capitalise on for intrusions. The attacker may take advantage of the weak security aspects of an application or software. So as a responsible user, post content carefully and intelligently. Social media cannot be made free from risks. Manoeuvre as if the content is a public property and refrain from sharing anything that will put oneself as well as the contacts and those around at risk.

7.4 South Korean Malware Attack

Reports and specifications regarding the malware used on March 20, 2013 to attack South Korean have been vague and inconsistent. There are however, some varied versions from different organisations regarding the malware, named Dark Seoul. The attack strategy was as follows

- The infected file erases the master boot record (MBR) and other files.
- The malware was attached with an execution date and time and was designed to search machines having administrative connection to servers
- The targets were South Koreans
- The malware operates on multiple operating systems
- Simple design with potential for huge damage

While studying the risks, it was found that DarkSeoul was designed to escape the typical South Korean antivirus. This malware was designed as a low risk to U.S. Critical Infrastructure and Key Resources (CIKR), however, the operators should relentlessly continue the strategies to avoid infection and transmission of any type of malware that may attack their networks.

7.5 Defensive Measures

On the basis of the above mentioned parameters of attack, US-CERT began to work towards a robust network model that can withstand any future attack on their enterprise. The intention is to minimise damage and maximise the business functions as soon as possible.

- Educate users on the need to transfer important files to network shares to pave way for central backup.
- Ensure daily backups of all important systems including offline and online copies
- Frequent execution of data restoration from backups for integrity of available processes
- Set up emergency communication plans in case of non-availability of network resources.
- Segregate critical networks from business systems
- Identify critical systems and analyse the importance of on hand spares for faster service retrieval
- Absence of internal monitoring system will lead to compromise of management services and destabilise security controls. Ensure strong password policy
- Maintain the latest antivirus engines and limit the user's ability to install and use unwarranted software applications
- Have updated operating system patches
- Disable unwanted workstations and servers
- Check for suspicious attachments and delete them. Also scan all software downloaded from internet before running them
- Be cautious when using removable storage devices
- Limit the number of cached credentials for all portable devices
- When administrative accounts are compromised, malicious activity occurs.

8. Knowing Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is a method of communication that enable making phone calls through broadband internet connection in the place of the conventional analogue telephone lines. VoIP allows to call others who can receive calls via internet. VoIP is increasingly used communication alternative for consumers. It is expected that VoIP is set to gain further popularity given the trend of decreasing broadband service rate. With the increasing usage of VoIP, expect an increase in threats to the user too. VoIP threats are almost similar to those on the internet. However, newer risks, tricks and unique IP telephony attacks are evolving.

8.1 VoIP configurations

- **Routers**

These instruments allow using the typical phone to make VoIP calls. They are linked to cable/DSL modems and enable attaching the conventional telephone. After configuration with an appropriate VoIP provider, these units do not require a special software or connection with computer. The number can be dialled and can be spoken through the phone. An adapter can be used to place calls when travelling, given the availability of broadband internet access.

- **Adapters (USB)**

These devices use conventional phones to make VoIP calls. A simple ordinary phone is attached to the standard modular phone jack. Once connected, the software places calls.

- **Software-controlled VoIP applications: "softphones"**

These are software applications, also known as softphones that enable to make VoIP phone calls straight from PV using headset, microphone and sound card. The applications and services help users to talk to other people who can access similar service.

- **VoIP phones**

A VoIP phone resembles an ordinary telephone but links right to a computer network unlike a phone that connects to a phone line. A devoted VoIP phone may include a phone and a base location that links to the internet or may work on local wireless network.

8.2 Requirements and Availability

One should be accustomed to the demands, supplies and possible service restrictions of VoIP service before changing to VoIP as a means of communication.

Requirements

VoIP connects to the Internet through an ISP, a VoIP service to expand to traditional landlines and VoIP software to make calls. It should be noted that Digital Subscriber Line (DSL) internet service make use of traditional phone lines for internet connection.

Availability due to power outages

During a typical electricity shut off, VoIP becomes unobtainable because VoIP devices (computers, routers, adapters) rely on a power source to operate. Traditional phone lines work during such a power shutdown, which is deemed a major plus in an emergency. It is recommended to use an unhindered power supply (UPS) with a VoIP installation for operating during a power outage.

Availability due to bandwidth

VoIP communication function only using a high-speed (broadband) internet connection for reliable functionality. A typical broadband connection is prone to service disruptions or deprivation of quality which is due to internet traffic.

8.3 Threats / Risks

VoIP faces similar threats that is characteristic to any internet application. Internet users are already used to the nuisance of email abuse by way of spam and phishing attempts. VoIP opens up yet another route for certain annoyances like abuse, spams and phishing attempts, which causes spam via internet telephony (SPIT), spoofing and identity theft. Additionally, the privacy of VoIP interactions can be questioned.

Spam over internet telephony (SPIT)

There will be annoying telemarketing calls and spams typical to any telephone user. However, a concept called spam over internet telephony has emerged which has exposed to the user to large volumes of unsolicited calls and spam voice messages.

Spoofing

It is possible for an attacker to deceive an unsuspecting user. By establishing a bogus caller ID into an ordinary VoIP call, the receiver trusts the incoming call. He may unknowingly disclose vital information. This is a VoIP version of phishing. Attackers with the pieces of details obtained may use it for faking identity of another.

Privacy concerns

The confidentiality element in VoIP is questionable. VoIP transmits unencrypted data over the internet. So it becomes precisely possible to collect VoIP data and start a conversation.

8.4 Steps to Protect from threats

Many of the methods used for safe VoIP are the similar for other internet applications. A few of the key steps of good personal computing are

- Mount anti-virus and anti-spyware series.
- Be wary about accessing files embedded in email messages or instant messages.
- Check the legitimacy and safety of the downloaded documents and new software.
- Ensure personal or financial data is secured.
- Create complicated passwords.
- Keep application software updated.
- Do not divulge personal information to unknown individuals
- Use encryption software for both installation and for the caller at the other end when using a software VoIP application

9. Protecting Aggregated Data

There is a reliance on collection and processing of huge amount of electronic data or aggregated data which in turn has initiated the evolution of sophisticated database software and hardwares with huge storage capacity. When organisations are storing and processing such vast data, they are vulnerable to serious threats such as attacks from cyber criminals, compromise of confidential data through illegal copying and altering of content and threat to the privacy and control of data. Such pervasive nature has serious implications on the day to day functioning of business such as inability to fulfil customer transactions, breach of trust, violation of laws pertaining to protection of data and exposure to law suits. These risks can be leveraged through judicious implementation of security practices. Organisations must attach tangible value to the data inorder to develop and execute security plans. The strategies developed should address all issues relating to vulnerability, breach of trust and its consequences, data manipulations, disclosure or loss, ramifications to organisations and plans for strengthening business-customer relationships.

Information security personnel are forever on their toes with the increasing number of cyber-attacks. With the decreasing cost of storage devices, enormous amount of data are being aggregated thus exposing it to risks. This aggregated data are compressed into electronic warehouses and are free from physical or operational demands of those using them. Aggregated data are vulnerable to both natural and man-made disasters. Information is the lifeline of any organisation. Therefore adequate precautions must to taken to preserve it from attackers. In information security, it is the data that prescribes the security necessities. In the run to protect data, organisations aggregate data in one or more logical locations and risk loss of control, use and ownership of data. Some of these problems and issues are as given below

9.1 Replication and Persistence

Aggregated data, when left unguarded, can be easily duplicated, shared, reformed and damaged. Just as a physical object that is created and destroyed easily, aggregated data too should be laced with the same attributes. However, this is impossible given the ease with which they can be replicated

9.2 Ownership

Another group of parameters question the ownership and guardianship of aggregated data. Continuing the likeness with a tangible object, the proof of identity of those who own and operate should be bounded and well understood. In reality, aggregated data rarely has responsible owner. Aggregated data has ever changing ownership and custodianship because of the simplicity with which electronic data is shared and duplicated.

9.3 Transformation

Aggregated data undergoes constant change. As far as electronic content is concerned, change is inevitable. Data is treated, scrutinised and aggregated to produce information. There is a continuous conversion of data into data because organizations use fresh data within a given context and yields information and intelligence. The question of ownership is lost in this transit.

9.4 Valuation

It is difficult to attach a monetary value to the data. The worth of the aggregated data to an organization can be ascertained if the person answerable to the organizational process recognises and approves on what exactly is being valued. Valuing aggregated data considering its unique characteristics, is vital for ascertaining the risks, the effects and thus can calculate the necessary investments in securing strategies and security arrangements.

Know the Risks and Effects- understand what would happen if

- Customer details are revealed
- Brand loses credibility due to data leakage
- Confidential data is stolen by rival
- Organisation is labelled incompetent in terms of privacy and data securing guidelines
- Network crashes due to data compromise
- Cannot identify data compromise

Once the organisation finds answers to the above, they can work on details such as money to invest, the area to which protection should be maximised and degree to which risk should be quantified. Organisational resources that are gravely affected due to security compromise are trust, ability to offer and fulfil customer needs, stakeholders' identity and privacy and ability to be compliant with legal regulations. There is an immediate impact on the organisation when security is threatened.

10. Protection Principles for huge Volumes of Aggregated Data

10.1 Comprehend the Information

The primary step in shielding anything is to comprehend its contents. For aggregated data, this includes knowledge of what information are available, where it is available and in what form. Ascertaining a required level of protection also need an understanding of the safety demands, its proprietors and custodians and likely risks and impacts. The owners and custodians must be aware of the worth of the data they possess. The potential impact of the data to the organisation reveals the value. Once the worth of the data and the extent to which risks can disturb the organisation or individual are ascertained, a meaningful profile can be designed against which management and security panels can be applied.

10.2 Apply realistic Management Doctrines

Adopt a set of universally accepted management doctrines in defining what defence strategies are suitable to protect aggregated data. Organizations can adopt principles to choose, infer, rank, organize, and underline policies, approaches, plans and actions. To be operative, principle assortment and Analysis should line up with organizational goals. The principles relevant to protecting and securing aggregated data are Accountability, Adequacy Awareness Compliance Measurement Response and Risk Management. Regulations are chosen to meticulously moderate peril and their performance is periodically measured and studied. Remedial action for risk mitigation are established and implemented after each assessment.

10.3 Application of Reliable Security Measures

In sync with management principles, a good set of usually followed security processes protect the organization's aggregated data. The areas that require protection of all kinds of information including aggregated data are

1. **Information Security Strategy**: The strategy incorporates and defines the organization's information security package, comprising of all the actions and operations that are implemented to ensure the mission's existence.

2. Information Security Policy: Information security policies are the accumulation of regulatory principles which the organization defines in order to set the standards of behaviour for using information properties and its effects, including aggregated data.

3. Security Structure and Design: Security structure and design is the tangible and rational execution of the organization's security schemes, policies, guidelines and techniques. It is the organization's methodological implementation of security pattern throughout multiple strata of the technical arrangement.

4. Incident Management: Incident management can be viewed as the organization's measures for recognising, recording and reacting to suspected security incidents and desecrations.

5. Partner Management: Partner management practices and activities ensure that vendors and service providers behave in the manner that assist the existence of the parent organization.

6. Emergency Planning and Disaster Recovery: Emergency planning and disaster recovery guides the measures and movements taken by the organization to continue the standard functioning of various activities when confronted with significant or hostile interference.

7. Physical Security Management: Physical security is a module of the inclusive protection plans, especially for concrete aggregated data assets such as hardware, software and media.

8. Information Technology: Information technology security is the array of practical instruments which the organization installs to enable and implement policy, principles and procedures.

9. Audit and Monitoring: Monitoring and auditing examine and scrutinize the extent to which the organization's strategies are being employed and surveyed. Monitoring activities are the roadmaps by which the organization systematically verifies its security system for flaws and susceptibilities and pledges suitable actions wherever necessary.

10. Liability Management: Liability management decides the procedural and functional vulnerabilities in the technical arrangement where aggregated data is located and how to proactively lessen the faults. Liability assessment is a defensive monitoring movement where systems and networks are checked for known technical flaws or faults.

11. Software License Agreements: Disregard at Your Own Risk

End User License Agreement or EULA is a legal bond between the user and the software publisher. It elaborates on the clauses and circumstances for using the software. For example, it might insist on installing the software on only a single computer for personal use. It might also state that by agreeing to terms, the user also agrees to third-party interference or permit other users to access the computer. When refused to accept the terms and conditions of the EULA, the software cannot be legally used.

11.1 Importance of EULA

EULAs encompasses a number of items that need to be seriously considered before installing the software. The following facts about EULA should be noted.

1. EULAs are legally binding- though the legality of EULAs can be challenged mentioning about the hidden terms and conditions, the user is bound to enter into a legal agreement by accepting the terms.

2. EULA restrict the software use- restrictions like the number of computers in which it can be installed, prohibiting software testing and publishing results and prohibiting reverse engineering are placed upon the user.

3. EULA demand agreeing to certain terms- force the user to use all bundled modules of a software bundle even those produced by third party publishers and permission to monitor the internet activity and sharing of resources.

4. EULA cannot be sued for damages- includes clause that restricts the user from suing the publisher for any damage incurred.

Pay attention to the following terms and conditions imposed in EULA as it may affect the online security.

- permits the third parties or publisher to monitor the internet activity
- permits the third party or publisher to gather personal details
- permits the software publisher to use computing resources
- binds the user to the terms of EULAs governing third party software modules

The following recommendations can be followed to protect from security and privacy issues related to EULA

11.2 Read the EULA before installing the software

Though it is boring to read through the entire list of conditions, it will definitely spare from hassles in future and is the only means by which the user understands the privacy and security issues he might encounter by assenting to the EULA's terms. Always ensure that the terms and conditions are understood. Contact the software publisher with any queries and clarification about any specific points. Software publishers often display their EULAs online.

11.3 Consider the software publisher.

When in doubt about the publisher, assess the EULA covering its software with extra attention. Publishers having good reputation are less probable to participate in fraudulent business practices like strange, ambiguous or masked clauses and conditions in the EULAs that dictate the use of their software. However, a company's credible business reputation is not a justification for skipping to read EULA. The good corporate status should not deter from reading and understanding the terms and conditions that govern its software. When handling softwares by unfamiliar publishers, review EULA with extra care. Be vigilant if the software is added with any new software from third party publishers

11.4 Beware of firewall reminders when installing software

During setting up of software, there may be firewall reminders asking for certain access to pass. This needs to be carefully scrutinised. Review EULA to understand why such a prompt must be encouraged. Ensure that the software requires changes only for normal operation. For example, if EULA requires monitoring and access to specified directories, tread with caution. In the case of bundled software, EULAs may request for permission to monitor and access directory which may not be included in the primary software's EULA. These EULA conditions may exist in the third-party software EULAs. Firewall prompts may indicate that bad software has been shoved into the software package for installation. When in doubt regarding firewall conditions based on reminders got during setting up of software, look up the software's user or installation guide. Proceed when reasonably convinced about the legitimacy of an appeal.

11.5 Beware of "open" or "free" software, mainly peer-to-peer (P2P) file-sharing software.

Seldom is anything genuinely free. Assess the EULA to check out what is required for installing the software and analyse the effect of this on the security of the computer and its contents. Many "free" software programs, like the file-sharing programs, regularly ask for a non- payable fee for their use. This non-payable fee is elaborated in the EULA and elaborates what is needed in return for using the software. This may be in the form of compulsory installation of modules that threaten security and secrecy.

11.6 EULAs, Security and Privacy

Privacy and security issues emerge from overlooking EULAs or by consenting to EULA terms that exposed users to hazards. The risks can also arise from poorly fared software business contexts in which the primary software publisher is unsuccessful in verifying its partners' software for worms, security matters and agreement with its EULA. The risk that is invited when consenting to definite EULA terms is not restricted to one's own data or device, but can also cover other computers and data linked to the network.

11.7 Observing Software EULAs

EULAs and bundled software can associate and generate security problems. Sometimes the malware that the user unintentionally installs verifies all of the Internet behaviour, containing the normal web browsing history in addition to the activity performed via secure sessions. Therefore, always scrutinize and assess any EULA that requires permission to monitor the online activity. The user should be ready to risk sharing intimate information to a third party. Even if the user is taking the risk of surrendering personal details to a third party, monitoring software can create bigger privacy and security issues. When weighing the impact of a EULA on privacy issues, think beyond the bigger confidentiality and security issues that the software might pose.

11.8 File-Sharing EULAs

Peer-to-peer (P2P) file-sharing programs are immensely widespread, but they initiate huge trouble for those related to safety and security. By consenting to the EULAs, the user permits third parties to monitor the internet activity and which in turn is shared with advertisers. Unknown people too, get the opportunity to access the directories on computer. There are popular P2P program that requires installation of bundled software that can convert the system into a dispersal passage for third-party software and content producers. The following are the perils associated with P2P file-sharing software:

- Increased susceptibility to Trojan horses and bugs
- higher risk to private details
- increased coverage to software errors that infect computer
- higher vulnerability to security flaws that can expose computer to exploitation

11.9 Resource Sharing EULAs

Sometimes, the service provider would change the terms of its EULA to support its other initiatives. Any request for permitting even restricted access of computer to another third party should be handled with extreme attention. Yielding to this kind of regulation may lead the third party to redesign the computer configurations in a manner that affects its security mechanisms. Also, consenting to the revised EULA will result in being accustomed to their computers connecting to other sources independently. The user may hardly decipher that the connection occurred as a result of a virus or spyware and not due to the existence of resource sharing software.

11.10 Third-Party Software and Surging EULAs

Mostly, the software purchased or downloaded is coupled with third-party software. Usually, the third-party modules establish their own EULA which may involve "downstream" third-party modules which are also covered by their own EULAs. This makes it difficult and confusing for the user to comprehend as to what is being agreed upon when installing the software and how all these EULAs affect the security and privacy of the computer. "Downstream" third- party software EULAs are many in number, making it difficult to comprehend the terms and conditions based on which the software can be used. It also puts up the question of the knowledge of chief software publisher about the downstream third-party software elements and their license contracts. It is imperative to be cautious when confronted with EULA that binds to the clauses of all third-party software EULAs. Do not make the mistake of assuming that the chief software publisher would have assessed the third-party EULAs and software.

12. Spyware

Spyware is a sort of malevolent software (malware) that gathers data from a computing structure without seeking the user's permission. Spyware has become more pervasive due to the fact that online attackers and conventional offenders use it as an instrument to commit felony against individuals, industries and governments. Spyware causes monetary loss, thereby reducing consumers' trust in online transactions and their inclination towards modern electronic commerce. To combat its widespread use, spyware should be made less lucrative for the offenders who make it available. Contemporary solutions that battle with spyware look at searching, stalling or eradicating it. Spyware can seize keystrokes, screenshots, validation permits, private email ids, web form data, internet practices and a host of different private information. The document obtained is often handed over to online assailants who make money by selling it to those who need them or use it for executing fraudulent activities. Spyware is widely used by online invaders, advertising organizations, structured crime and reliable insiders.

Online Attackers- the basic motive is to steal personal information for committing financial crimes or to sell it those who commit such crimes or for identity theft

Marketing Organizations- look for personal details, browsing habits and trend related content to undertake marketing movements like spam and spim messages, browser popups, home page stealing.

Spying by a reliable Insider- Trust-worthy insiders are those who have direct contact or contact to computer systems for valid reasons. A reliable insider is someone, say an employee, who uses spyware to gather confidential business secrets that can be sold in the illegal market, or used for blackmail or used to seek more valuable data for a later use.

Another example of the trusted insider group includes intimate members of the family or close relatives spying to catch inappropriate behaviour.

Spyware can observe almost every activity or data associated with computing milieu. This is not just restricted to contents on hard drives but also comprise of back-up data.When spyware operates on a computer system, every data is within the access of a malicious programmer. Most vulnerable data include internet habits, email and contact information, windows-protected Store data, clipboard data, keystrokes, screenshots and network traffic.

12.1 Effects of Spyware

Spyware leads to decreased confidence and trust in online business dealings. Just like the problem of fake currency in the real market, spyware destabilizes online economy. Consumers' willingness to indulge in online money transactions will be reduced fearing personal financial loss. In the run to control the risk, vendors and financial institutions often resort to additional authentication and loss anticipation modules at an exorbitant operational cost. Though financial organizations shield an individual from loss incurred from online fraud, the cost incurred to govern loss-prevention programs are ultimately borne by consumers by way of higher service fees, interest rates or highly priced goods and services. Consequently, growth rates nosedives, costs rise up and demand shrinks.

Depending on the type of spyware modules installed on a system, users may go through substantial performance loss. Systems under spyware attack exhibits reliability issues. Affected systems may become unstable, causing significant loss of output and data. Mostly, spyware is impossible to erase without an exhaustive understanding of its working methods or by taking extreme measures such as erasing the entire system. For the system to function all over again, the operating system and applications are required to be reinstalled.

Spyware risks the systems even in future as the malicious content is capable of controlling the system over a long period of time. The profound information gathered by spyware often includes log in IDs that can be utilised for future access to the affected system. People seldom change the login name and password and use it for many other systems or accounts. Therefore, these stolen contents can be used to break into uninfected systems. This opens up newer avenues for committing additional information theft or malware installation. Spyware also threatens the computer by installing backdoor access systems. These backdoors help the malware operator to regulate the system, to command the system, to download and operate indiscriminate applications. Attackers can access many infected systems without infecting a single system.

12.2 Common Spyware Systems

There are numerous versions of malware. Many versions of malware act basically as spyware, while many other malware series contain spyware components.

Some commonly observed forms of spyware and their operating traits are as follows:

Browser session hijacking- This type of spyware works to alter the user's browser features. Though hijacked spyware can be embedded in various ways, the motive is to change the way the browser operates so that the user is driven to sites of the malware creator's choice.

These redirects usually take the users to promotional sites that can earn the hijackers some charges when visited by users.

Browser Helper Objects- Browser Helper Objects (BHOs) are a component of Internet Explorer that can be misused by spyware, but they are difficult to be detected. BHOs can read all files, network assets and anything that can be accessed by the user who introduced Internet Explorer. Malicious BHOs can be embedded via a stand-alone dropper. Droppers are a distinct type of malware that give other malware to the user they intend to affect. They usually function by installing spurious files on the device and then alter the system in a manner permitting the newly written malware files to be operated. Another popular social engineering method is to flood the user with recurrent pop-up appeals to connect the software. It stops only when the user exits the site or consents to install the constituent. Once installed, it can run freely, download and connect to new malware or even change browser settings permitting malware to be downloaded without a warning or interaction with the user.

Cookies and Web Bugs- Cookies are bits of data kept on the user's system by a web server. During successive visits, the web server can recover these cookies. Often, cookies are utilised for keeping user authentication, favourites and other kinds of user-related information. The cookies can then be used to find parts of the user's browsing preferences. Web bugs are HTML components, which often exist like image tags that regain data from a remote web site. While the image is not noticeable to the user, it can give valuable information about the operator on request. Web bugs are mostly implanted in web pages and HTML-enabled email messages.

Fake Antispyware Tools- There are applications existing on some internet sites that claim to be spyware detection or deletion tools, when they are actually spyware.

Autonomous Spyware- Usually, autonomous spyware work as a distinct process or introduces itself into other processes operating on the system. This type of spyware mostly gets activated when logged onto the computer and can reach the contents of the computer. As autonomous spyware is just a malicious application, it can be premeditated to execute almost all types of spying activities.

Bots- A distinctive group of malware known as a bot or zombie is one of the most potential malware threats. Bots are remote operated proxies run on the system. Bots are mostly controlled distantly via Internet Relay Chat (IRC). Once a system is corrupted using a bot, it becomes a component of a bot network (botnet) It is used in sync with other botnet members to undertake the functions ordered by the bot creator or bot herder.

12.3 Precautions

To prevent the spreading of spyware and other malware, it is pivotal to exercise caution to distrustful actions on the computer and to adopt safe computing techniques. While a few spywares are positioned by taking advantage of the loopholes in operating systems or applications, most of them still banks on social engineering to mislead the user into installing or operating the malware. Always exercise restraint when downloading stuff from public web sites, newsgroups, fast messaging sessions or even when accessing email attachments from known senders. Identity on the internet cannot be verified. Usually, assailants and their malware imitate acquaintances of the target victim to persuade them into running the malicious code.

Do not rely on unknown or known high-risk sources- Be cautious when surfing unknown websites. Dangerous sites comprise those with many popups, persistent requests to operate browser components and those with content that is oriented on illegal titles such as software hacking.

Read the fine print- On deciding to work on an application obtained via the internet, ensure that the entire license or privacy documents related to the software are thoroughly understood. Lengthy or hard to understand agreements should be considered as a warning sign and installing the application should be reconsidered.

Exercise attention when loading applications- Software installation sets sometimes exploit a user's tendency to ignore the minute details and simply consent to the default "checked" alternatives. If the default options are thoughtlessly clicked and prompts are disregarded, there can be loading of spyware, adware or other applications that are undesirable. Read the instructions thoroughly to stay safe.

Keep an updated operating system- Keep systems and applications updated with security– related patches including patching up of the operating system and all installed applications.

When running Windows XP, install service pack 2- Windows XP service pack 2 includes several structures that will prevent spyware. It encompasses pop-up blocking, an upgraded automated latest process, an improved host firewall and security options for protection from drive-by installations of malware.

12.4 Antivirus and Antispyware Tools

Installing credible antivirus and antispyware tools and keeping them up to date is pivotal to computer security and is an important caution-strategy.

Browser Settings

Configure the browser to block active content and other potentially infectious content can go a long way in increasing online security. Disabling active content features block many threats. However, it is also prone to damage many modern web sites and applications. But, the richness of the browsing experience will be diminished. One ideal browser configuration strategy that is used to mitigate the risk related to active content, while still allowing authentic sites, is enabling the use of Internet Explorer security zones.

Email Configuration

In an email program, design it to send and exhibit email using simply the text, instead of html. This eradicates most of the threats arising out of embedded script, web bugs and other HTML-enabled systems executed by attackers. But merely using plain text decreases the functioning of some features. Further, many email clients are now providing the facility to disable scripting and block pictures until a user initiates action to show them.

Operate your Computer securely

Nearly all spyware needs a spark to start itself when the user is operating the computer. Spyware often works in combination with system start-up, user login or when specific applications, say an internet browser or any other software is introduced. Every application that spontaneously starts is not malicious, however, it is better to recognize which software is genuine. One ideal mode to find and deactivate spyware on the system is to inspect the software loaded on the computer and ascertain whether it starts up automatically or not. Windows XP Service Pack 2, a new feature, supplemented to Internet Explorer, permits some management of browser add-ons. Using this instrument, reviewing, enabling and disabling add-ons like BHOs and ActiveX, controls can be undertaken. This tool is available

in Internet Explorer, below the heading ‘Internet Options’on the Programs tab, when clicked on the ‘Manage Add-ons’ button.

13. Virus Basics

Virus- A computer virus is defined as a program that attacks by initially affecting files and the system locations of a computer or network router's hard drive, and then generating duplicates of itself. Though some viruses are benign, others are malicious and can infect data files or simple files. Earlier, viruses used to spread when people shared portable media, but now viruses are primarily transferred via email texts. Unlike worms, viruses need an action initiated by the user, like opening an email attachment or visiting a malicious web page to be transferred to other sources. The virus is a program and is capable of doing anything that a normal program does. Some viruses are created to intentionally destroy files whereas others are designed to be transferred to other computers.

Worm- A worm is a sort of virus that can be transmitted without human involvement. Worms transfer from one computer to another and affect memory and network bandwidth, which leads to malfunctioning of the system. Worms permit attackers to gain access to computer remotely.

Trojan horse- A Trojan horse can be termed a computer program that encompasses a virus or other fatal program within it. A Trojan horse can be a platform that is supposed to do one activity when, in fact, it carries out a malicious activity on the computer. Trojan horses can be packed into a software that is downloaded for no charge or as attachments in email messages. Primarily viruses, Trojan horses and worms are triggered or activated the moment an attachment is opened or when a link contained in an email message is clicked. If the email client has scripting option, then it is likely that a virus is transferred by just opening a message. It is best to restrict to the HTML that is available in email messages. The ideal way to see email messages is in plain text. Most users get affected due to opening and operating unknown email attachments. Always ensure that the contents of the file are known before resorting to opening. Contact the sender of the mail before opening the attachment to cross check if it was indeed sent by them. If the user receives a mail or message with an attachment from an unknown sender, delete them immediately without opening the attachment. Opt to check email messages in plain text rather than in HTML. This goes a long way in tackling virus infection.

13.1 Tips to protect from viruses and reduce their effect

- Load anti-virus software from a reliable vendor and update it frequently.

- More than just scanning for viruses on a periodic basis, load an "on access" scanner and configure it every time you start your computer.

- Run a virus scan before opening any new program or file that likely contain an executable code, including packaged software which is bought or downloaded.

- Be wary of accepting files or clicking links that people send within online communities.

- Ensure that there is a back- up data to avoid loss of valuable data due to virus infection.

14. Using Wireless Technology Securely

The recent years have seen wireless networking becoming more accessible, reasonably priced and easy to use. Home users are deploying wireless technology in amazing numbers. When working on wireless technology or those considering to move to wireless, it is mandatory to understand the security issues one may encounter.

14.1 Threats in Wireless Connections at homes

Those intending to shift to a wireless connection at home, should consider the security issues that rise when internet connection is opened to the airwaves.

The following sections elaborate on some of the risks to home wireless networks.

14.2 Piggybacking

When wireless network is not secured, anyone having a wireless-activated computer within periphery of the wireless access plug can intrude on the internet using the wireless connection. The normal indoor broadcast distance of an access point is 150 to 300 feet. Outdoors, this distance can reach up to 1000 feet. Inability to protect wireless network could possibly make the internet connection accessible to a many other users. Doing so is laden with a series of problems:

- Service violations- when the sum of connections exceed the permissible limit set by the internet service provider
- Band width shortage- illegal users may exhaust the bandwidth and make the connection slow
- Abuse by malicious users- other users may commit illegal activity which will be tracked to the genuine user
- Monitoring the internet activity- malicious users may watch the internet activities and try to steal sensitive credentials
- Direct attack on computer- illegal users can access the contents of the computer, install spyware and establish control over the computer

14.3 War driving

War driving is a particular type of piggybacking. The broadcast distance of a wireless access point enable internet connections to be accessible beyond the home limits even extending to the streets. Tech savvy computer experts drive around cities with a wireless-equipped looking for unsecured wireless networks. This exercise is called war driving. War drivers expose the details of the location of unsecured wireless networks on web sites to operate their illegal online activity.

14.4 Unauthorized Computer Access

An unprotected wireless network in symphony with unsecured file sharing is a deadly combination. These are the perfect conditions for a malicious user who could gain entry to any manuals and files capable of being shared.

14.5 Protecting Home Wireless

It is clear that the security problems related to wireless networking are inevitable. For this, there are certain measures to be taken for protection.

Keep the Wireless Network hidden -Wireless access points display their availability to wireless-powered computers. However, everyone need not know the presence of a wireless network at home. To keep the network hidden to others, check the access point’s user guide for directions on deactivating identifier broadcasting.

Change the name of the Wireless Network- Most of the wireless access point systems have a default name. The default names used by various manufacturers can assist in gaining illegitimate access to the network as the names are widely known. While renaming the network, choose a name that would be difficult to be predicted by others.

Encrypt the Network Traffic flow- the wireless access point system should be permitted to encrypt traffic flow movement between the system and computers. Encrypting wireless traffic enables transforming it to a programme that can be comprehended by computers with the correct hint to that programme.

Change the Administrator Password- ensure that the administrator password is changed to protect it from unauthorised access. This is because the already set default password is widely known by others and permits easy unauthorised access.

Use File Sharing with Caution- always use password protection for anything that is being shared. If the file sharing option is unnecessary, disable it.

Keep the Access Point Software Patched and Up to Date– always update the system software or patches for periodic healing of bugs.

Check the Internet Provider’s Wireless Security Options- check the customer assistance section of the provider’s website for getting information about securing home wireless network.

14.6 Public Wireless Threats

A wireless-enabled device are convenient even outside our home or work environment but they are vulnerable to many security threats.

The following are a few of the security risks that one encounters when working on a public access point.

Evil Twin Attacks

In an evil twin attack, the attacker collects details about a public access plug. He establishes his own device to impersonate the actual access plug. Gullible users will connect using the stronger, fake signal. The attacker can then view any content the victim transfers over the internet.

Wireless Sniffing

Almost all public access points are not secured leading to sensitive communications or transactions prone to threat. The malicious users can use “sniffing” devices to acquire sensitive information of the users like financial details or passwords

Peer-to-Peer Connections

Many laptops can create informal networks when they exist near one another. These networks create computer-to-computer connections. An intruder with a network card designed for ad hoc mode and operates on similar features as your computer, he can easily get unapproved access to personal files

Unauthorized Computer Access

Just as with unprotected home wireless networks, an unprotected public wireless network having unsecured file transferring capability can have disastrous consequences. Under these conditions, an intruder could gain entry to any documents and files permissible for sharing.

Shoulder Surfing

In public wireless spaces, the intruders are always on the vigil to steal sensitive information.

A public place is itself an opportunity for the intruders. If close enough, they can just look over when typing. They can peer through binoculars or by just watching, can steal all confidential, personal information.

14.7 Secure Wireless Networking in Public Spaces

Using the internet via a public wireless access plug is laden with serious security issues which is multiplied by the incompetence to govern the security setup of the wireless network. The following steps can be taken for protection.

14.8 Be vigilant when online in public space

In public place, it is an unsecured, unencrypted network connection. So be vigilant when online. The probability that another user, available on the network, watching the online activity is high. So avoid online financial activities, online shopping, sending email and typing passwords or credit card details.

14.9 Connect Using a VPN

Many establishments have a virtual private network (VPN) which permit their staff to connect safely to their network, when not in office. VPNs encrypt connections at the sending and receiving points and drive out movement that is not encrypted.

14.10 Disable File Sharing

File transferring in public wireless spaces is far riskier than on home wireless network. This is because the wireless-powered laptop is more likely to be near to other computers run by unknown people. Also, many public wireless networks have peer-to-peer networking. To prevent attackers from reading sensitive files, deactivate file sharing feature when linking to a public wireless access plug. Seek help to study the ways to disable file transferring.

14.11 Be Alert of Your Surroundings

When using an open wireless access plug, be cautious of the surroundings. Check if others are

using their computers in close vicinity. Check if someone can get a view of the screen. If an internet connection is not necessary, deactivate wireless networking totally. If there is a necessity to connect, use caution and follow the protection steps.

15. Data Backup Options

All computer users should always back up the critical data they are keen to store and safeguard, to safeguard it from loss or corruption. Keeping just a single backup file may not be sufficient to protect information.

15.1 Remote Backup – Cloud Storage

The recent widespread expansion of broadband internet facility has enabled cloud storage accessible to a broad range of computer users. Cloud service users access the internet to connect to a common group of computing assets like networks, servers, storage, applications and services owned by a cloud service provider. Remote backup services can safeguard data from natural catastrophes or critical malfunctioning of local devices infected by malware. Additionally, cloud services give ‘anytime- anywhere’ connectivity to data and applications on availability of an internet connection. But, the cloud’s reliance on the internet can hamper communications between the user and the cloud. Further, there are no world-wide accepted yardsticks, platforms or codes for cloud computing. Cloud customers are ignorant about the service provider’s cloud framework or its dependability and users lose control over their own data. Cloud service providers encrypt user data, thus protecting from access of critical information. Shared clouds pile up an individual’s data along with many other users’ data in the same cloud framework, thus posing a potential security threat. Prior to entrusting vital data to a cloud service provider, analyse the service contract for security practices.

15.2 Internal Hard Disk Drives

Hard disk drives stock data on a revolving magnetic tray read by a moving read/write head. Almost every desktop and laptop computers use their internal hard drive to pile up data required to operate as well as store the user’s primary files. Secondary systems and backup servers stock information on internal hard drives. Hard drives are rewritable and can be used to perform rolling backups. Having main file copies and its backup files on the same internal hard drive permits updating backup files and maintaining a simple file structure, all without the additional hassle of acquiring any other storage device. However, rolling backups can slowly disseminate corruption or malware in the basic files to the backup files. Also, if internal hard drive is spoiled, stolen or infected, both primary and backup files will be lost. Additionally, the computer always uses the internal hard drive. Therefore, the more backup files, lesser the space on computer. Backup files kept on the internal hard drive are equally susceptible to destruction and corruption as the primary files. Ironically, internal hard drives are only as safe as the computers that stocks them.

15.3 Removable Storage Media

Storage media that permits the user to connect and disconnect from computer are a more reliable backup alternative than the computer’s internal hard drive. Physical extrication of backups from computer keeps data secure, both from online fraudsters and power fluctuations. Removable media are portable and work on most computers. Their availability in a wide variety of storage dimensions and rates help find the one that fits the requirements and budget. Further, they are also reusable. But, their portability makes them vulnerable to loss or theft. Rolling backups may move infection from the primary files to the backups. Removable storage media gives direct regulation over data. So, the user himself is responsible for protecting that data.

15.4 Types of Removable Storage Media

External Hard Disk Drives -External hard drives are similar to internal hard drives, but they are handy and easy to load. But, they are still prone to destruction and are huger than solid-state storage of similar capacity.

Solid-State Storage - Solid-state storage, also known as flash drives, USB flash drives, thumb drives, SD and micro-SD cards, memory sticks and solid state drives (SSD), are popular portable storage media. Solid state devices are small, resistant to shock and access data quickly. USB drives are small and can be plugged-and-played on computers. Solid state media are rewritable. They do not pile data magnetically and so are free from the danger of corruption.

Optical Storage - Optical storage media, such as CDs, DVDs and Blu-ray discs, accumulate information on reflective discs read by a moving laser head. Storage capacity differs greatly from the available optical media, that is, from 682 megabytes on CDs to 9.4 gigabytes on DVDs and up to 50 gigabytes on Blu-ray discs. Most computers have some kind of internal optical disc drive available. Content on non-rewritable discs cannot be inadvertently deleted or receive infections or malware from other sorts of primary files.

Magnetic Tape- A digital tape system contains a tape deck, individual tapes and sometimes, a tape auto-loader. Individual digital tapes can offer storage of over one terabyte, or approximately a thousand gigabytes and are inexpensive. Once loaded, digital tape systems are equipped for very less user interaction and process data swiftly. The reusable tapes power the rolling backups and are less prone to infections than hard disks

Floppy or ZIP Disks- Floppy disks and ZIP disks preserve data on spinning magnetic trays, almost like hard drives. The biggest disadvantage is their low storage capacity compared to other storage devices, and the drives that read them currently out-dated and are not manufactured, thus making floppy disks and ZIP disks obsolete.

15.5 Choosing the Best Backup Option

Before choosing a data backup option, evaluate the pros, cons and security issues of each device, financial resources, requirements such as the size of back up data, security for sensitive data and accessibility of data. Home users having little data can opt for preserving primary files on the hard drive of their system or remote storage. People or small traders who have large amounts of non-sensitive data can keep their files on their hard drives or servers. Large businesses or organizations may choose to keep one backup copy onsite and another offsite either through a dedicated data service or on the organization's private offsite servers or digital tape system.

16. Disposing of Devices Safely

16.1 Why protect data

After buying a new computer system, notebook, tablet or any other gadget that is necessary, latest and enjoyable, we may decide to dispose off the old equipment. We may choose the device for recycle, or to be given to a friend or contribute it to a charity. However, it is most important to safeguard the information on it from becoming public. But erasing information can be cumbersome. Systems protect us from losing vital information and help in getting it back when we delete a file. Similarly, others who get hold of the thrown off device can get back the data, too. We need to be extra cautious in removing contents from the computing systems before disposing them to prevent from revealing private information, such as financial credentials, social security figures, health information and personal details and passwords. Otherwise, we may face threat of identity theft. Similarly, computing devices engaged for business purposes, when not disposed properly, will reveal sensitive information such as customer and employee details. Business reputation, customer confidence, exposing financial details are all revealed. Removing data from computing devices is called clearing. Clearing is a procedure of media wiping that prevents data to be repossessed back by disk or file recovery services. It must withstand keystroke recovery attempts from standard input and from data scavenging devices.

16.2 Techniques for erasing Information

There are three ways of erasing information from computing devices. They are deleting, overwriting and physically damaging the device containing vital information.

Deleting

Deleting information is least effective. It removes pointers to information on computer, but does not erase the information as such. Deletion method that we normally use when operating on computer, like shifting a file to the trash or a recycle bin, or selecting "delete" from a menu, is not a reliable method. In spite of trash being emptied, the information still exist there. It can again be reclaimed.

Overwriting

Overwriting is operational on all computing systems. It puts unsystematic data on information, which is impossible to be retrieved because it has already been eradicated. While professionals agree on the process of such random or unsystematic data, they differ on the number of times overwriting should be done to ensure safety. There have been debates regarding this. While some say that doing it once is enough, others stick on to doing it at least three times, after which "zeroing" the drive needs to be done. There are many overwriting mechanisms available. A few of them are open source and are freely available. Darik's Boot and Nuke (DBAN) is a widely used tool that completely erases the drive. Eraser can be used to safely erase individual files. Refrain from using these tools if it is a solid-state drive. Secure Erase and Parted Magic are effective on every drive, especially when we select "secure delete." Parted Magic supplies many options along with its data sanitizing gears.

Physical demolition

Physical demolition is the best way to thwart others from reclaiming vital information. Of course, physical destruction should be carried out on the device only if we do not intend to donate it to others. Specialized services will degenerate, burn, dissolve or crush the computer drive and other devices. If for some motive, we do not wish to seek someone else's assistance, it is possible to damage the hard drive ourselves, by puncturing it with nails, making holes into the device or even hammering it. However, do not ever burn a hard drive or insert it in the microwave oven or dispense acid on it. Some crushers are armed to damage flexible devices such as CDs and DVDs. If we smash or shred the device our self, make the pieces tiny enough to avoid data from being rebuilt. Magnetic devices such as tapes, hard drives and floppy disks can be ruined by degaussing, that is, showing them to a very strong magnet. Degaussing is more applicable and feasible for businesses than individuals, due to the expenditure that will be incurred. It should not be carried out if someone else requires the use of the device because degaussing damages not only the data but also the “firmware” that assists the device to operate.

16.3 Destroying data in Mobile Phones and Tablets

Although the step by step process for erasing all information from mobile phone and tablet vary for each product and model, the general procedure is the same.

1. Take out the memory card, if the device uses one.

2. Take out the SIM (Subscriber Identity Module) card.

3. Under the Settings option, select Master Reset, Wipe Memory, Erase All Contents and Settings. This may require entering a password, if the set has one, or seek assistance of an approved dealer that sells the device for a factory-set password.

4. Manually damage the memory card and SIM card or stock them in a protected place. Memory cards and SIM cards can be used again in a phone that has the same model.

5. Ensure that the account has been closed and/or moved to another new device.

17. Conclusion

Computing devices permit huge amount of data at our disposal. When we discard a gadget or donate it to someone else, there is a threat of revealing information to people who are not supposed to have it. A haphazardly disposed gadget can have a big deal of useful and sensitive information. The data preserved electronically on such discarded devices can be safely prevented from landing into the wrong hands by following the above processes. We have to be a responsible user of such technology stuffed gadgets to protect ourselves and environment from unrepairable damages.

18. Common Perils of Using Business Apps in the Cloud

The cloud is the theory of distantly held IT services, labelled cloud apps, delivered by a seller. These sellers are called cloud providers. Normally, cloud apps presented by cloud givers include email, calendar, files, online storage, sales, customer support and many more. Incorporating business apps in the cloud has widely accepted benefits- saving money by paying for the required IT computing possessions only, ramping up or down computing resources quickly without capital investment and spreading the influence to employees and users anywhere in the world.

18.1 Common Perils of the Cloud

There is no total control- When IT services are bought from a cloud provider, there is no comprehensive regulation over the computing resources that the business requires for functioning. Situations like cloud provider winding up business or changes its services or prices is not discussed. Sometimes, there may an outage resulting in severe damages that can impact business, customers and economy as a whole.

Getting trapped with one supplier- Every cloud provider is different in terms of their platforms using different hardware, software, configurations and settings. Therefore, suddenly shifting from one supplier to another can be impractical, even when using the same app. The user might get trapped with one supplier and migrating will be really difficult. An app may behave differently on another cloud. Switching from one provider to another will be practical only when there is more standardization across cloud providers.

Data is preserved by someone else- When using a cloud provider, the data is stored and secured by the cloud provider. Despite the provider being more equipped to buy the latest security software and assistance, it may not protect data as the user does. Business vitals can be lost or mishandled and data may be stalled because of a government action. Confidential data can be stolen when a scrupulous intruder takes the encryption code required to connect to data. Further, cloud provider is likely to be located in a different location from business physically. The locations of these data centres have legal repercussions and are bound by the laws of the countries in which they operate. If the data centre gets entangled in a criminal case, the laws governing business in the country and the state where it is located, enforce stringent laws on data control. Also, many countries have stricter laws for encryption.

Security is managed by someone else- Usually, cloud providers have avenues that are more protected than our own because they are richer in resources compared to measures taken by organizations for security. Cloud providers accommodate numerous customers’ data on the same servers and operate a huge bulk of data than even large organizations. So they are the most desirable pawns for cyber criminals.

Beg for information- Unbelievably, some of the popular cloud providers do not permit their customers to undertake audits. Some cloud providers offer the audit results to their customers.

However, not all audits are identical.

18.2 Risk Relief in the Cloud

Be Aware

Have awareness about the job roles of staff members in the organization. Keep watch over their actions related to work on clouds providers. Staff may purchase some services easily on credit or through free trials, unaware of the threats.

Be an intelligent consumer

Select suppliers who agree to contracts that enable effective functioning of business. In particular, ensure that the cloud provider’s security regulations are sufficiently in sync to business-needs. Almost all cloud-provider license agreements have clauses that protect the cloud provider from being responsible for loss to a business arising due to a service outage. Always negotiate on those terms. If possible, negotiate contract terms that outline requirements for the computing assets. Also, be aware of the data location and the laws that apply to those locations.

Accommodate the correct people in cloud decisions

Supplier selection, monitoring and management skills are mandatory to manage suppliers involved in the business. Find experts in supply-chain management. Accommodate both corporate leaders and IT professionals in decision making regarding choice of cloud provider.

Be cautious

Establish trust with cloud givers vigilantly. Begin by using the cloud for unimportant services and evaluate the provider's performance. Over time, build trust depending on what services to seek from cloud. Be choosy about what to control and what to be maintained on the cloud. Match the risks and benefits of preserving the apps and data on systems versus the pros and cons of transferring it to the cloud. Instead of being controlled by the cloud provider, the keys can be governed by business to ensure that the data be recovered.

Observe the cloud provider's actions

Identify methods to confirm that the terms of the SLA are honoured. Keep updated of the security related conditions incorporated by the cloud provider and its skill to be abreast with developments in cyber-crime. Ensure that there is right to use to the same information if the service was in held in the organization itself. Include conditions in the SLA that highlights the right to access the information without resistance.

Be prepared for cloud outages

All cloud providers have shut downs. Clarify about the cloud provider's disaster contingency plans. Investigate a novel approach where a private cloud works along with a public cloud. Also opt for a multi-public cloud execution of a service through two or more cloud providers.

Cloud apps for business are a big boon but just ensure that the risks and its effects on business and industry are completely understood. Use an augmentation approach and form trust slowly by monitoring cloud provider's activities and have a contingency layout for cloud outages.

19. The Basics of Cloud Computing

Cloud computing is a payment-based service where we can acquire networked storing space and computer assets. The cloud makes the required information accessible from anywhere, any time. While a conventional computer setup requires physical presence in the exact location as data storage device, the cloud makes that step redundant. The cloud removes the need for physical existence at a given location as that of the hardware that stores data. The cloud giver can both possess and accommodate the hardware and software required to operate the applications. This is especially supportive for companies that can ill -afford the exact amount of hardware and storage space. Small companies can approach the cloud to preserve data, thus eliminating the cost of purchasing and preserving memory devices. A business can look for more space or decrease their subscription as per their business growth. The only prerequisite is that there is a need for an internet connection for accessing the cloud.

19.1 Types of clouds

There are diverse categories of clouds that can be subscribed depending on the requirements.

1. Public Cloud – Accessible by any customer who has an internet connection and connectivity to the cloud space.

2. Private Cloud - A private cloud is set up for a definite group or organization and restricts connectivity to only that group.

3. Community Cloud - A community cloud is one that is mutually divided among two or more organizations who have identical cloud specifications.

4. Hybrid Cloud - A hybrid cloud is fundamentally an amalgamation of at least two clouds, where they are a mixture of public, private or community clouds.

19.2 Selecting a cloud provider

Each cloud provider aids in a specific function, providing users with limited control over their cloud based on the type. When choosing a provider, compare the needs to the cloud services available. The cloud prerequisites will be influenced by how the space and assets associated with the cloud be used. For personal home use, there is a need for a different type of cloud and a provider compared to the cloud for business. Depending on the technological needs storage space can be bought from cloud provider.

There are three types of cloud providers that we can subscribe to

1. **Software as a Service** - A SaaS provider gives subscribers right of entry or access to both resources and applications. In a SaaS agreement, the subscriber has no control over the cloud.

2. **Platform as a Service** - A PaaS provider gives customers rights to use the elements that they need for developing and operating applications on the internet.

3. **Infrastructure as a Service** - An IaaS agreement, as the name suggests, deals predominantly with computational arrangement. In an IaaS document, the subscriber completely sub-contracts the storage and resources, such as the required hardware and software components.

The cloud provider has the least power in an IaaS system than with a SaaS agreement.

The subscriber has the autonomy to choose the degree of control over his/her data and kinds of services that is required from a cloud provider. For example, people operating small business cannot meet the expense of purchasing and storing entire hardware and software necessary to stay in the competitive market. By subscribing to an arrangement as a Service cloud, he can run the new business with the computational sophistication of a larger company, by paying only for the storage space and bandwidth that is used. Assessing the current computational resources, the level of control expected, the financial situation, and the future of business must be taken into account before signing up with a cloud provider. After a detailed analysis of the requirements, research into different cloud providers will give better insights of which is suitable.

19.3 Security

The information contained on the cloud is often seen as treasured to individuals with mischievous intentions. There are plenty of personal information and likely secret content that people preserve on their computers and these information are now shifted to the cloud. This makes it imperative to recognize the security precautions that the cloud provider offers. Likewise, it is important to take personal measures to secure data. The foremost thing to be considered is the security measures that the cloud provider offers. The security parameters vary from one provider to another and among the different types of clouds. Points to be noted are the decoding methods the providers offer, methods of protection for the actual hardware that houses data, the availability of backups of data, firewalls etc.

Most cloud providers have standard terms and conditions for different range of subscribers. The home user may not have any concession in their cloud contract. A small business user is likely to have slightly better negotiation related to the terms of their agreement document with the provider. It is pivotal to choose a cloud provider that gives the security of data as the major priority. In spite of being extra careful with personal data, merely subscribing to the cloud will make security to be compromised and transfer control to an external source. The distance between the subscriber and the geographical location of data forms a hurdle. It may generate more room for a third party access to information. However, to enjoy of the paybacks of the cloud, we will have to forego direct control of data. Most cloud providers will have enough expertise on how to manage data and keep it secure. A cloud provider is equipped with more resources and proficiency than the average user in securing their computers and networks.

The cloud provides numerous alternatives for the everyday computer users- large and small businesses alike. It unbolts the lock to the domain of computing to a wider range of users and enhances the comfort by giving links through any internet connection. However, the increased ease has its drawbacks. The cloud is a gullible victim for any malicious activity and has serious security issues because it can be operated through an unprotected internet connection. When using the cloud, ensure that protection is given to the information and the person responsible for access on the cloud is trustworthy. Additionally, subscribers should possess knowledge of alternatives in terms of what type of cloud is suited, what type of provider will be most convenient and the reputation and responsibilities of the providers before signing up.

20. Office and Home Router Security

Home routers are an inseparable part of the modern tech savvy society with its widespread use in work from home options, home business, school assignments, social networking, personal financial management and entertainment. The internet service provider delivers preconfigured, ready to use wired or wireless routers. Often, the home users are unaware of the configuration settings and do not perform any additional or advanced settings. But, the default configuration of the home routers provide no security features thereby exposing the networks prone to attacks. Small organizations use these same routers without proper implementation of security measures due to lack of funding for advanced IT infrastructure.

20.1 Security Apprehensions

The in-built configurations of home routers expose them to security issues. Home routers, being directly operational from the internet, are easily noticeable and in many cases are misconfigured. These traits help an intruder find the most suitable victim. The wireless feature, integrated into many of these devices, is an addition to the already existing threat. The following mitigation steps are aimed at intensifying the security of home routers and decrease the susceptibility of the internal network against attacks from external fronts.

1. Alter the default login username and password- Makers already set default usernames and passwords for router devices and provide the same to customers to configure the system. These default usernames and passwords are familiar to attackers. Hence, they should be renamed during the preliminary router loading. A strong password is one which is a mixture of letters and numbers and it should be set.

2. Modify the default SSID- A service set identifier (SSID) is an exclusive name that recognizes a specific wireless LAN (WLAN). All wireless devices on a WLAN must adopt the same SSID to interact with each other. Makers fix a default SSID that normally identifies the maker or the actual device. An attacker can make use of the default name to recognize the device and any loophole related to it. Users usually fix the SSID to their organization name, the location, their own name, etc. This enables the attacker to ascertain their specific business or home network depending on an SSID certainly associated with their name.

3. **Configure WPA2-AES for data concealment-** Wireless Equivalent Privacy (WEP) is a security rule created to offer data secrecy like authentication and encryption, but it has serious lapses. WEP was outdated by the 802.11 standard implemented as Wi-Fi Protected Access (WPA), which has a newer form, WPA2. WPA and WPA2 offer powerful authentication and encryption through certain keys. WPA and WPA2 is available in personal and professional versions.

4. **Restrict WLAN coverage-** LANs are innately more secure than WLANs because of the protection provided by the tangible structure in which they exist. WLAN coverage mostly extends beyond the boundaries of the home or organization. This paves way for spying by intruders outside the network limit. Therefore, restrict the broadcast coverage area when securing WLAN.

5. **Switch off the network when not operational-** The crucial point in wireless security measure is closing the network. This will undoubtedly shield the network from outside attackers from violating it. While it may be unfeasible to turn on and off the devices repeatedly, this approach can be adopted during travel or long offline time period.

6. **Deactivate UPnP**- Universal Plug and Play (UPnP) is a convenient feature that permits networked devices to effortlessly identify and launch interaction facilities with each other on the network. Though the UPnP feature simplifies initial network configuration, there is also a security threat. For example, malware within the network can break into the router to allow entry of intruders.

7. **Elevate firmware**- Just like software on computers, the router firmware, which is the software that controls it, must have latest updates and patches. Many of the updates take care of security issues that impacts the network.

8**. Use static IP addresses or restrict DHCP reserved addresses**- Most home routers are designed as Dynamic Host Configuration Protocol (DHCP) servers. Deactivating DHCP and redesigning clients physically is the most feasible alternative, but it may be unrealistic based on the extent of network and support staff.

9. **Deactivate remote management**- Deactivate to stop attackers from starting an association with the router and its configuration via the wide area network (WAN) interface.

10. Disable remote upgrade- This feature permits the router to work on the WAN interface for TFTP traffic which can affect the security of the router firmware. Therefore, best option is to deactivate it.

11. Deactivate DMZ- The router's demilitarized zone (DMZ) establishes an isolated network open to the internet. Disable this feature when not operating it.

12. **Disable redundant services**- As with any computer system, deactivate all redundant services in order to prevent the routers from getting exposed.

13. **Deactivate ping response**- The ping response feature is normally disabled by default. When this feature is activated, exploration on the router becomes hassle-free. It permits router to react to ping directions sent from the internet and may expose the network to attackers.

14. Empower router firewall- Most home routers have an in- built firewall feature. Make sure that this feature is enabled and meticulously designed to let only genuine users and services to connect to the network.

15. Logging- Activate router logging and periodically evaluate the logs for vital details regarding infringements, spying, attacks, etc.

16. Observe the wireless traffic- Always check the wireless traffic for any scrupulous network access by carrying out usual log analysis of the devices that have operated the router.

17. Administrator workstations- Ensure that any administrator workstation built for managing the router is on a reliable portion of the network to avert outsiders spying and gathering details about the network.

18. Immobilise bridging and use network address translation (NAT) - Home routers segregate the interior network from the internet by means of network address translation (NAT). NAT gives private IP addresses to every device connected on the network.

Some routers encompass a facility that lets them to function as a channel between two networks. This component can be operated for linking segments or devices on the same intranet to the internet via a routers routable IP address. Deactivate this feature when not operational, to prevent the threat to the router.

21. Governing for enterprise security

The previously unknown knack of security is now a compulsory and inevitable part of functioning of business. Governing for enterprise security means considering security as a non- negotiable obligation of business. If an organization's management does not set up and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, accomplished or continued. United States and European Union passed many laws in the last decade that mandate organizations to implement security measures. The Sarbanes-Oxley Act of 2002 mandates public companies to lay regulations for the accuracy of financial data. The Gramm-Leach-Bliley Act ensures that financial institutions protect customers' personal data. The Health Insurance Portability and Accountability Act (HIPAA) directs the medical industry to protect privacy of personal health care. The Federal Information Security Management Act ensures that agencies comply to security controls. To achieve a viable capability, organizations must ensure that enterprise security be a predominant concern of the leaders who are at a governance level, and should not be given to other organizational roles that lack the authority, accountability and means to act and impose compliance.

More than 30 U.S. state governments have issued laws that necessitate companies to openly confess any security gaps that result in the negligent revelation of state citizens' personal data. This is terrifying for those associated with a business. If a company reveals that have been irresponsible by losing its customers' data, its reputation could be tarnished and it could be unable to find new customers, its stock prices may fall and it could lose income and their current customers. These can be considered business issues rather than security issues. Probable risks to businesses are numerous ranging in impact from minor to tragic. Risks can be in the form of natural calamities, terrorism, power shut down, hackers, mischievous insiders, user faults, computer viruses, worms, internet malware, phishing emails and social engineering. Further, threats that are deliberately created rarely target IT systems in particular. However, they still face huge security repercussions. Because of its potential impact on various business functions, security is not the sole domain of the IT department alone. Security is a central competency for business frontrunners, who must now ensure smooth operation and continuity of business, despite all kinds of threats. This includes at least an overview of major security concerns. Thus forewarned, people in position will be better equipped to have productive discussions about how to safeguard business resources from internal and external attacks. These discussions might take place among the leaders who are in a variety of management roles.

Security threats and as well as its solutions are enterprise-wide. Leaders do not need to be experts who are proficient in every individual threat, but they do need a superficial knowledge of threat. Some efficient managers do impart an active and knowledgeable role in risk mitigation, working in collaboration with IT section and other departments to execute proactive policies to safeguard sensitive data. Others may participate in security risk reduction in a more restricted way. Some managers may delegate risk mitigation to other personnel. Unfortunately, this is not how security concerns should be handled. Everyone in an organization, particularly top executives, must take responsibility for security. Because leaders are accountable for more critical judgments than most other employees, their obligation is even greater.

22. Safeguarding Home Network

Computer security is the process of averting and identifying illegitimate use of computer. We use computers for everything from making online payments for utilities, banking, investing, shopping, communicating with fellow users through email or for social networking programs. Although our communications are not top secret, we do not wish unknown people reading email, using our computer to attack others' systems, sending bogus email from our computer or investigating personal content stored on the computer particularly, financial statements.

Prevention steps help stop scrupulous elements from accessing computer system. Detection helps to find if there is an attempt to intrude into system. Intruders, also known as hackers, attackers or fraudsters will wish to gain control of computer in order to fuel assaults on other computer systems. Having control of computer helps them to make their true geographical location and identity invisible, as they launch attacks, mostly against high-profile computer systems. Intruders can track the users on the computer, create damage to computer by re-formatting the hard drive or alter the entire data. Unfortunately, intruders are constantly identifying new loopholes to exploit computer software. The intricacy of software makes it ever more challenging to systematically test the safety of computer systems. Also, some software applications have pre-set features that sanction other users to operate the computer unless the settings are altered for more protection.

To know more about security aids, let us understand a few terms. Firewall is a system or a combination of systems that establishes an access-restriction policy between two networks. In the home networks background, a firewall usually takes any one of two forms

- Software firewall - specific software running on an individual computer
- Network firewall - a dedicated device responsible for protecting one or more computers.

Both types of firewall encourage the user to outline access rules for incoming connections to the computers they are protecting. Some also provide the facility to control the kind of facilities the protected computers can access on the Internet. Most firewalls proposed for home use are available with pre-defined security guidelines from which the user can choose and customize the policies depending on their specific needs. There are numerous antivirus software packages that work in many ways. The similarity between them is that they all look for forms in the files or memory of the computer that specify the possible presence of a known virus. Antivirus packages know what to expect through the use of virus profiles. The efficacy of antivirus software is depended on getting the updated virus profiles installed on the computer so as to detect new viruses.

22.1 Computer security issues to home users

Information security is apprehensive about three attributes namely

- Confidentiality - information should not be available to wrong people
- Integrity – data should be edited only by those individuals who are sanctioned to do so
- Availability - information should be made available for access to those who need them

Some security threats arise from the likelihood of planned exploitation of computer by intruders using the Internet. Other risks are hard disk failures, theft, power shut downs, etc. The bad news is that it is impossible to be ready for every potential risk. The good news is that some simple steps can be adopted to reduce the chance of getting affected. The most common methods adopted by attackers to gain control of home computers are listed below.

- Trojan horse programs
- Behind the door and remote administration programs
- Rejection of service
- Being an arbitrator for another attack
- Unsafe Windows shares
- Mobile code (Java, JavaScript, and ActiveX)
- Cross-site scripting
- Email hoax
- Email-laden viruses
- Invisible file extensions
- Chat clients
- Packet sniffing

In addition to the risks related to connecting the computer to the Internet, there are a number of threats that the computer encounters even if it is not connected to network. Most of these risks are well known, however, it is important to understand suitable practices associated with minimising these risks. This may also help decrease vulnerability to the network-based threats.

Disk failure- Hard disk damages are the common cause of data damage on personal computers. Steady system backups are the lone viable option.

Power failure and fluctuations- Power problems like surges, blackouts and brown-outs can do physical harm to the computer, either by a hard disk crash or a damage to the electronic parts of the computer. Common modification method is to use uninterruptible power supplies (UPS).

Physical theft- The act of stealing a computer results in the loss of privacy, integrity and availability of data. Regular system backup helps in recovering the data. But backups, by themselves, cannot guarantee confidentiality. Cryptographic tools are existent that can decode data embedded on a computer's hard disk.

22.2 Preventive Actions that home users can adopt to safeguard their computer systems

The CERT/CC recommends the following actions to home users:

- Seek help from system support personnel when working from home
- Install virus protection software
- Load a firewall
- Do not open unknown email attachments
- Avoid running programs of unknown origin
- Deactivate invisible filename extensions
- Keep all applications, including the operating system, patched
- Switch off the computer or disconnect from the network when not required
- Disable Java, JavaScript and ActiveX if possible
- Deactivate scripting features in email programs
- Ensure there are regular backups of critical data
- Make a boot disk, in case, the computer gets damaged or affected

23. Identifying and Evading Email Scams

Email is a useful and influential communication tool. Unfortunately, it is also a perfect instrument vulnerable to scammers and other malicious individuals to carry out activities for luring potential victims. The scams range between old-fashioned procedures to phishing schemes using an amalgamation of email and bogus web sites to coax victims into exposing delicate information. To avoid falling a prey to these scams, one should comprehend what they are, how they look, how they operate and ways to prevent them.

23.1 Identify email scams

Email has made the game easy for scammers. The suitability and secrecy of email, enable to easily contact millions of people instantly, facilitating the scammers to work in bulk. Scammers need to trick only a small percentage of people they email, for their stunt to gain returns. The email scams have been in existence for a long time. In fact, most of them are merely reprocessed scams. It is easy to identify such bogus emails. The list of the most common types of email content are related to fake business opportunities, work from home options, health and fitness scams, fast money schemes, investment options, guaranteed loans and credit schemes. The discount offer scams contain mostly endorsements of cheap versions of expensive software and are unbelievable offers.

The advanced fee fraud schemes are quite detailed in nature and lure the victim into a fake plot to acquire huge amount of money. These scams are easily recognizable from the names and the subject line itself as they look like an African connection because most of these originate from those regions. Social engineering is an approach for soliciting sensitive information from people, which they normally would hesitate to disclose, or by prompting an action which people would not usually perform, by kindling their inquisitiveness or inclination to trust. Phishing emails are designed to resemble as if they have originated from an authentic organization. These emails attempt to trick people into visiting a fake web site, to either download malware or divulge sensitive personal information. The culprits of phishing scams meticulously design the bogus web site to look like a genuine one. The bogus site will look amazingly real and will present an online form seeking information like bank details, account number, address, online banking username and password, all the vital data an intruder requires to steal the identity and break-in to bank account. Bogus communications looks like they have been sent from banks, credit card companies, financial institutions and IT Department.

Trojan horse email offers the promise of something that people might be usually interested in, like an attachment enclosing a joke, an image or a patch for a software vulnerability. Once opened, however, the attachment performs the following actions. -create a security threat on computer and open a backdoor for illicit access, load software that records keystrokes and transfers the logs to an attacker, install software that observes and records online connections and activities, provide the connectivity to files, convert the computer into a “bot” which the attacker can operate to send spam, initiate attacks or spread the virus to other computers. Many viruses spread by scanning all email addresses on a corrupted computer and then mailing themselves to these addresses. The following suggestions can reduce the chances of becoming a victim of these scams.

Filter spam- Most email scams begin with unwelcome marketing email. Take steps to avert spam from getting into mailbox. Look into the help file for email application or service to understand what to do to filter spam.

Do not entertain or trust unsolicited email- Do not spontaneously trust any email sent by an unknown individual or organization. Always refrain from opening an attachment from unsolicited email. Most essentially, never click on a link sent in an email. Skilfully designed links can lead to bogus web sites set up to trick into revealing private information or downloading viruses, spyware and other malicious software. Spammers may also use a modus operandi in which they send unique links to each individual spam email. By tracking which links are asked for on their web servers, spammers can identify which email addresses are useable and are more likely to be target victims for repeat spam attempts. Be aware that even email received from a known address are risky. Many viruses transfer themselves by searching the target computer for email addresses and moving themselves to these addresses by disguising as an email from the user of the corrupted computer.

Be cautious in dealing with email attachments- Email attachments are widely utilised by online intruders to get a sneak-peek virus onto the computer. These viruses enable the scammer to get access to important information from the computer, infect the computer to enable it to be susceptible to additional attacks and abuse. This is then converted into a 'bot' for future use, attacks and other online crimes.

Install antivirus software and keep it updated- Always install antivirus software on the computer that has a programmed update option. This will ensure that there is the most up-to-date protection possible against viruses. In addition, ensure the antivirus software chosen encompasses an email scanning feature. This will protect computer from email- borne viruses.

Load a personal firewall and keep it up dated- A firewall may not be equipped to prevent scam email from entering into mailbox. But, it may help protect if a virus-bearing attachment is inadvertently opened. The firewall, also helps in preventing outbound movement from computer to the intruder. When personal firewall notices a suspicious outward communication from computer, it could indicate an infected program being installed on the computer.

Configure email client for any potential threats- There are a numerous ways to configure email users to make them less vulnerable to email scams. For example, organising email program to view email as "text only" will prevent scams that misuse HTML in email.

Learn the Email Policies of the business partnering organisations- Most organizations doing businesses via internet have laid out policies regarding communication with their customers in email. Many, for instance, will not demand account details or personal information via email. Familiarising with the policies of the organizations can help spot and avoid phishing scams. Always refrain from sending sensitive information via unencrypted email.

24. Securing Your Web Browser

Nowadays, web browsers like Microsoft Internet Explorer, Mozilla Firefox and Apple Safari are loaded on almost every computer. Since the use of web browsers are so frequent, it is important to design them securely. Mostly, the web browser got along with an operating system is not installed in a safe default configuration. Insecure web browsers result in a variety of computer complications, including spyware being installed without the user's knowledge and intruders establishing their power over the computer.

Preferably, computer users should assess the issues from the software they operate. Many computers are bought with already loaded software. Irrespective of whether they are loaded by a computer manufacturer, operating system maker, Internet service provider or by a retailer, the foremost step in evaluating the susceptibility of computer is by identifying what software is loaded and the manner in which programs interact with each other. Unfortunately, an average user is ill- equipped to carry out such a detailed analysis.

Vulnerable web browsers are always prone to risks from attackers. It has been seen that new software weaknesses have been exploited and aimed at web browsers, through the use of compromised or malevolent websites. This problem is catapulted by some of the following factors.

- Users have the penchant for clicking on links without evaluating the consequences of their actions.
- Disguised web address that navigates to an unexpected site
- Web browsers being configured with less attention to safety features
- New security threats are often revealed after the software is designed and bundled by the manufacturer.
- Computer systems and software packages may be loaded with supplementary software, exposing to a number of susceptibilities
- Third-party software are not equipped for security updates.
- Many websites force users to activate certain features thereby exposing the computer to additional risk.
- Many users do not have knowledge to organise their web browsers safely.
- Many users are averse to enabling or deactivating utility as needed, to ensure security of their web browser.

24.1 Web Browser Structures and Perils

It is imperative to apprehend the functionality and structures of the web browser. Installing many web browser options may risk security. Vendors mostly activate functions by default to advance the computing performance. But these functions result an increased risk to the computer. Attackers direct their efforts to misusing client-side systems, that is, user's computer, through various exposures. They make use of these vulnerabilities to overpower computer, steal data, damage files and use the same computer to attack other computers. Attacking web browsers is a low cost method adopted by attackers. An attacker can design a scrupulous web page that will load Trojan software or spyware to steal data. Instead of vigorously targeting and attacking compromised systems, a scrupulous website can inertly infect systems as and when the site is clicked. Another way is to send a malicious HTML document to victims. In such cases, the moment the email or attachment is opened, the system gets infected.

A few web browser features and allied risks are discussed.

ActiveX is a technology that Microsoft Internet Explorer operates on Microsoft Windows systems. ActiveX permits applications or portions of applications to be applied by the web browser. ActiveX has been inundated with various risks and execution issues. One main issue with using ActiveX in a web browser is that it enhances the risk surface. Loading any Windows application gives the chance of new ActiveX panels being loaded.

Java is an object-oriented programming which serves the purpose of developing active content for websites. Various implementations of the JVM contain risks that allow an applet to dodge these constraints.

Plug-ins are applications proposed for practice in the web browser. Plug-ins are identical to ActiveX controls but cannot be implemented separately from a web browser.

Cookies are files located on the device to stock data for precise websites. Cookies may contain browsing history or may even contain authorisations for operating the site. Cookies are useful for uniquely recognizing visitors of a website. If a website uses cookies for validation, then an attacker can gain illegal entry to that site by procuring the cookie.

JavaScript, also known as ECMAScript, is a scripting language that is capable of making websites more collaborative. There are guidelines in the JavaScript standard that limit specific features from operating local files.

VBScript has the credit of being one more scripting language that is distinctive to Microsoft Windows Internet Explorer. Though VBScript and JavaScript are alike, it is not popularly used in websites due to its incompatibility with other browsers. The facility to operate a scripting language like JavaScript or VBScript permits web page authors to augment a noteworthy number of features to a web page. However, this very facility can be misused by attackers.

24.2 How to safeguard Your Web Browser

Some software dimensions that provide functionality to a web browser such as ActiveX, Java and Scripting may also present susceptibilities to the computer system. These susceptibilities may shoot from bad execution, poor design or an unprotected configuration. For these reasons, it is inevitable to recognize which browsers support each feature and the risks associated. Some web browsers allow full deactivation of these technologies, while others may allow f activation of these features on a per-site basis. Always visit the vendor's website of each browser and study about it. If a vendor hides the necessary details on securing the browser, contact the vendor and request for more details. Many web browsers can be loaded on the computer. Therefore, it is mandatory to safely restructure each web browser loaded on computer. One benefit of having numerous web browsers is that one browser can be utilised for secret and sensitive functions such as online banking, while the other can be used for normal web browsing. Operating on multiple browsers can leverage the chances of vulnerability in a particular web browser or website. Web browsers are periodically updated. So, depending on the type of the software, the dimensions and options may shift or alter.

25. Recovering from a Trojan Horse or Virus

Given the widespread number of viruses and Trojan horses navigating the Internet at any specific moment, it is most important to take the most needed proactive measures to secure the computer system. Once the user finds out the specific virus that has harmed the computer, visit the concerned website and download an antivirus tool. The choices being limited because of being in oblivion, the user can adopt the given steps for securing the system and its files.

1. **Contact IT support**- contact The IT helpline and notify them as soon as possible and work based on their directions

2. Cut off computer from the Internet-Based on the type of Trojan horse or virus that has affected, intruders can also gain entry or view personal information and may even convert the computer into a bot to launch attack on other computers. This activity can be stopped by switching off the Internet connection. The ideal way to achieve this is to physically disable the cable or network connection or phone line.

3. **Back up all important files**- It is always advisable to have a stand-by or back up of required files. If possible, assemble all the required documents, images and files and write them onto a CD or DVD or transfer everything to another external storage device. Not to be forgotten, these files are not reliable since they are still potentially corrupt.

4. **Scan the machine**- Since the computer is loaded with a malicious program, it is best to scan the machine from a live CD instead of using an antivirus program installed in the past. Most antivirus products provide this feature. Another substitute is to make use of a web-based virus deletion service. After installing the software, take up a complete scan of the system. The first scan itself will, hopefully, erase the malicious files from the computer.

5. **Reinstall the operating system**- If scanning has failed to clean computer, the next feasible alternative is to format the hard drive and reload the operating system. Although this remedial action will lead to complete loss of all programs and files, it is the only alternative available to guarantee that computer is safe from intruder-amendments.

6. Restore files- once a backup of the files is made, it can be restored. Before placing the files back onto the computer, test them with anti-virus software to ensure that they are virus-free

7. Protect the computer- to safeguard the computer from future attacks, remember the following

- Refrain from opening unknown attachments in email messages.
- Never click or follow unsolicited links.
- Have a latest anti-virus software installed
- Use an Internet firewall.
- Always secure web browser.
- Keep the system patched.
- Always be a responsible technology-user

Copyrights