Computer Cons

A Pinku and Dadaji

Series

Hackers design computer viruses

Pinku: Good morning Dadaji. Dadaji, can you check my computer it's not working since yesterday.

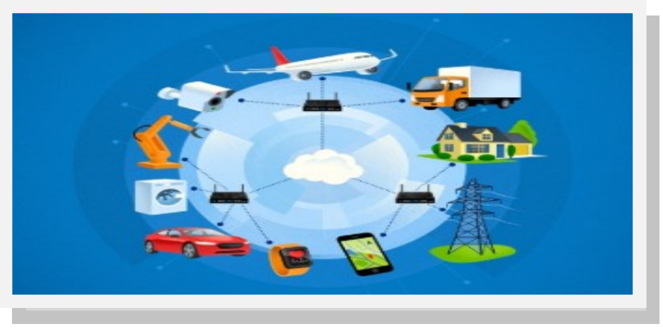
Dadaji: Good morning Pinku. Let me check… "After a while"… Pinku, your computer has lots of viruses. Hence, it is not working.

Pinku: Computer virus I thought virus is there only in human body which causes diseases.

Dadaji: Well! Yes there are viruses in computers also. However these are not live viruses such as viruses in your body let's say those viruses which cause common cold. Computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

Pinku: Hmm… what should I do to avoid such programmable viruses entering in my computer?

Dadaji: You should install "anti-virus "in your computer.



Your desire can fall you under trouble as you are inviting viruses

Pinku: And what is an anti-virus Dadaji?

Dadaji: Anti-virus is a software which will look out for virus threats, remove any it finds, and provide you with the ability to run ad-hoc full system scans.

Pinku: That's the reason my dad every week runs anti-virus scans to see if the system is affected or not.

Dadaji: That's a very good practice that your father follows. You should regularly do anti-virus screening on your computers to avoid computer infection. Now days even though most of the anti-virus programs come with auto screening options, you should regularly update the patches or software of anti-virus as day in and day out new viruses are spread through internet.

Pinku: Makes sense Dadaji. Any tips that you could give to protect my computer from being affected by viruses?

Creeper creeps across your computer

Dadaji: Yes. Check few of my tips below:

⇒ Should the worst happen, ensure you have a regular backup for all your files.

⇒ Never download programs from untrusted sites as viruses often get on your computer via an infected program.

⇒ Some viruses can be transmitted simply by previewing an email with infected images. View images from trusted sources.

⇒ Better purchase any anti-virus rather than relying on free anti-viruses available online.

⇒ Use a firewall which can block third parties from activating a virus on your computer.

⇒ Regularly update your Operating system to protect your computer from the latest threats.

⇒ Utilize Administrator rights. Admin rights prevent changes being made without your knowledge by forcing an Admin password to be required any time a change is made.

⇒ Pay attention to virus warnings and notifications. Your antivirus solution should provide you with notifications or warnings in one form or another. As soon as one appears, take it seriously, and take action.

Learn pros and cons of what you click on internet first

Pinku: Hmm... those were some knowledge helpful tips Dadaji. Can you give me some examples of nasty viruses?

Dadaji: Well there are several hundreds of them but you should know some of the aboriginal ones such as Creeper, iloveu, code red, Nimda, slammer, blaster, Commwarrior etc.

Pinku: What is the name of first virus Dadaji?

Dadaji: First developed in 1971, Creeper might well be the first computer virus. It infected DEC PDP-10 Computers that ran the TENEX Operating System. Once infected, the computer would display the message, "I'm the creeper, catch me if you can!" Self-replicating but not too dangerous, Creeper opened the door that the rest of this list walked through.

Elk Cloner is the first computer virus

Developed by Bob Thomas it was an experimental program that was self-replicating. The Reaper was later developed to delete this virus.

Pinku: Hmm... Which was the first virus to be known in history?

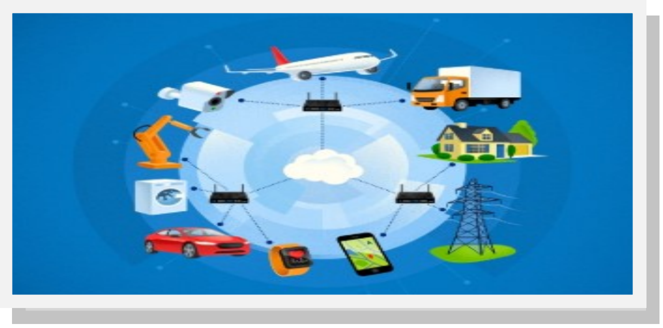
Dadaji: Well Pinku! Elk Cloner was the first computer virus to be known. In 1982, Richard Skrenta, then fifteen years old, wrote the virus for the Apple II operating system, which was stored on floppy diskettes. When a computer booted from a floppy disk infected with Elk Cloner, the virus would start, and would subsequently copy itself to any uninfected floppy disk that was accessed. Because computers of that time had dual floppy disk drives, and because diskettes were often passed around among friends, the virus was frequently copied. After contagion, every 50th time that a computer booted up, it would display the following text:

"Elk Cloner: The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes it's Cloner!



It will stick to you like glue

It will modify ram too

Send in the Cloner!"

Elk Cloner was not intended to cause damage, but was created as a practical joke. The adolescent Skrenta had a penchant for modifying programs so that they stopped working after some code-specified time period had elapsed, at that point displaying some joke text that Skrenta had written. Elk Cloner's capacity to copy itself (the major criterion of a virus) made it possible for Skrenta to continue to annoy his friends without requiring physical access. The virus is reported to have spread widely among his fellow students (and also to his math teacher), thus ensuring Elk Cloner's place in history. But this was more for home networks and among known friends.

Pinku: Practical Joke and with programming hmm...So, then which was the first widespread virus Dadaji?

You should know how to handle social media

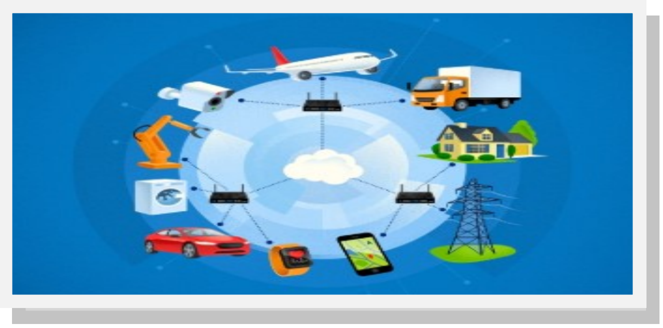
A Virus can replicate itself

Dadaji: The two brothers Basit and Amjad Farooq Alvi developed "(C) Brain" the first IBM PC virus to infect machines running pirated copies of a program they sold for physicians in Lahore (Pakistan). It is a boot sector virus similar to Elk. They had given their original telephone numbers and address to those who used pirated versions. The brothers were surprised to note that the virus was spread across US and UK from where they received calls to disinfect their machines. There was never any legal action, but the media response was explosive, and people from all around the world blocked the brothers' phone with furious calls. However, despite all the fuss their virus caused in the world, Brain was never bad for the brothers' business. Their company, Brain Net, is now one of the largest Internet service providers in Pakistan.

Pinku: I will remember the name Brain Dadaji. Tell me Dadaji are computer viruses always bad?

Dadaji: No Pinku Not at all! This statement will sound surprising to you. The first question that will come across in anyone's mind would be "How can computer viruses be good"? If we look the positive side of this, viruses can:-

⇒ Kill other viruses.



Con artist exactly knows the victims wishes

⇒ Encrypts the hard disk so that it cannot be used elsewhere.

⇒ A virus that can replicate on the network to perform some cleaning tasks.

Pinku: Yes Dadaji that makes sense. Can you let me know some bad viruses that shook the world?

Dadaji: Oh Sure! But before that you should know the types of viruses.

Pinku: Types of Viruses Oh! So you have types also in viruses...hmm...

Dadaji: Yes Pinku. Here are types of Computer Viruses that you should know about:

1. Boot Sector Virus: A boot sector virus is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks

2. Web Scripting Virus: A web scripting virus is a type computer security vulnerability through websites that breaches your web browser security.

Viruses can by-pass access controls

This allows the attackers to inject client-side scripting into the web page. It can bypass access controls; steal your information from your web browser.

3. Browser Hijacker: Browser hijacking is a form of unwanted software that modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser. A browser hijacker may replace the existing home page, error page, or search engine with its own.

4. Resident Virus: A resident virus is a computer virus that stores itself within memory allowing it to infect other files even when the originally infected program has been terminated

5. Direct Action Virus: A direct action virus is a virus that attacks or start to work immediately this can include nonviolent and less often violent activities which target persons, groups, or property deemed offensive to the direct action participants.

6. Polymorphic Virus: A polymorphic virus is a complicated computer virus that affects data types and functions. It is a self-encrypted virus designed to avoid detection by a scanner. Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.

Free is always minuses than pluses

7. File Infector Virus: A file-infecting virus infects executable files with the intent to cause permanent damage or make them unusable.

8. Multipartite Virus: A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously. Most viruses either affect the boot sector, the system or the program files.

9. Macro Virus: A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel or word processors such as Microsoft Word. When a macro virus infects a software application, it causes a sequence of actions to begin automatically when the application is opened.

10. Overwriting Virus: An overwriting virus is a malicious program which, after infection, will effectively destroy the original program code, typically by overwriting data in the system's memory.

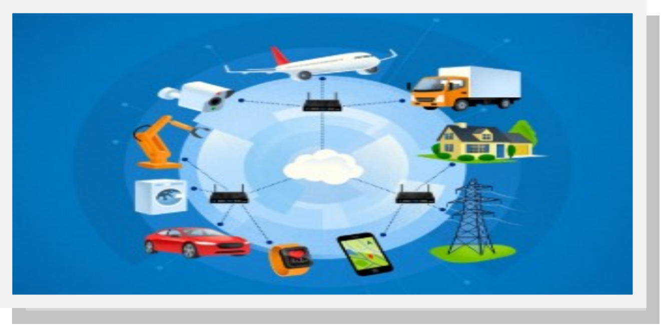
Virus can disable anti-virus

11. Spacefiller Virus: Also known as "Cavity Viruses", spacefiller viruses are more intelligent than most of their counterparts. A typical modus operandi for a virus is to simply attach itself to a file, but spacefillers try to get into the empty space which can sometimes be found within the file itself. This method allows it to infect a program without damaging the code or increasing its size, thus enabling it to bypass the need for the stealthy anti-detection techniques other viruses rely on.

12. File Deleting Virus: A File Deleting Virus is designed to delete critical files which are the part of Operating System or data files.

13. Mass Mailer Viruses: Mass Mailer Viruses search e-mail programs like MS outlook for e-mail addresses which are stored in the address book and replicate by e-mailing themselves to the addresses stored in the address book of the e-mail program.

14. Armored Virus: Armored Viruses are type of viruses that are designed and written to make itself difficult to detect or analyze. An Armored Virus may also have the ability to protect itself from antivirus programs, making it more difficult to disinfect.



Your files are important
keep them in secure mode

15. Stealth Virus: Stealth viruses have the capability to hide from operating system or anti-virus software by making changes to file sizes or directory structure. Stealth viruses are anti-heuristic nature which helps them to hide from heuristic detection.

16: Retrovirus: Retrovirus is another type virus which tries to attack and disable the anti-virus application running on the computer. A retrovirus can be considered anti-antivirus. Some Retroviruses attack the anti-virus application and stop it from running or some other destroys the virus definition database.

Pinku: Oh my god Dadaji so a many… what are the other type of creatures similar to viruses?

Dadaji: The other creatures are Worms, Trojans, Bots, spyware, Nagware, Ransomware, Adware, Shareware, Freeware, Spam, Crippleware/ Freemium, Donationware, Careware, Postcardware…

Malware is Malicious Software

Pinku: Can you explain each of these Dadaji?

Dadaji: Ok. Let's see each of these creatures in detail. But to understand each of these creatures you should know "what is malware".

Pinku: So what is Malware Dadaji?

Dadaji: Well! Malware (short for "**mal**icious soft**ware**") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. Though varied in type and capabilities, malware usually has one of the following objectives:

⇒ Provide remote control for an attacker to use an infected machine.

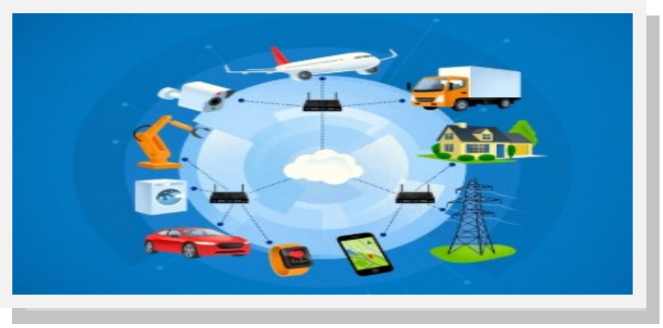
⇒ Send spam from the infected machine to unsuspecting targets.

⇒ Investigate the infected user's local network.

⇒ Steal sensitive data.

Pinku: So you are trying to tell me that virus is a malware and what about other creatures above are they malware too.

Dadaji: The definition of Malware as I have described you is malicious software. As long as the software program is intended for malicious jobs it is a malware. Viruses are a specific type of malware designed to replicate and spread and similarly all the other creatures I mentioned you are malwares.



Use a good anti virus to protect your PC from infections

Pinku: Understood Dadaji. Let's start with understanding worms.

Dadaji: Oh! Sure Pinku. A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. Computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge. Worms can modify and delete files, and they can even inject additional malicious software onto a computer.

Trojan is attached to a genuine program

Worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

Pinku: Are you aware of any famous worm Dadaji?

Dadaji: Yes Pinku. It's called Stuxnet. Stuxnet is believed to be prepared by US and Israeli agencies to curb Iran's nuclear expansion. Stuxnet was designed to hit only one, very specific, target; the computers that controlled Iran's nuclear facility in Natanz, where international authorities suspected the country was working on its secret nuclear weapons program. Stuxnet was programmed to make the uranium enrichment centrifuges spin faster than they were supposed to, causing them to get out of control to the point of damaging them. The malware was so well programmed that its victims could do very little to stop it. In fact, they didn't even know the outages and disruptions were caused by a computer virus. FYI this was the first cyber weapon developed in the world and it was a worm. It's a very interesting story to read. Do take some time out to research on stuxnet on internet.

Pinku: Oh! Sure Dadaji. Now to our next topic; what is a Trojan Dadaji?

Dadaji: Borrowed from the story of the wooden horse which Greeks used to enter the city of Troy, a Trojan similarly hides malware in what appears to be a normal file. Most Trojans are typically aimed at taking control of a user's computer, stealing data and inserting more malware on to a victim's computer. Trojans aren't just problems for laptop and desktop machines. They can also impact your mobile devices as well. Generally speaking, a Trojan comes attached to what looks like a legitimate program, however, it is actually a fake version of the app, loaded up with malware. The cyber-criminals will usually place them on unofficial and pirate app markets for users to download.

Do not invite hidden enemy by clicking something that you do not know

Pinku: It's good that you compared Trojans with story of Trojan horse to better understand. Thank you Dadaji... What are the types of Trojans Dadaji?

Dadaji: Here you go Pinku:

Trojan attacks from backdoor

⇒ Backdoor Trojan: A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer

⇒ Downloader Trojan: A Trojan Downloader is a malicious program typically installed through an exploit or some other deceptive means such as an Email attachment or Image

⇒ Info stealer Trojan: An information stealer (or info stealer) is a Trojan that is designed to gather information from a system. The most common form of info stealer gathers login information, like usernames and passwords, which it sends to another system either via email or over a network. Other common information stealers, such as key loggers, are designed to log user keystrokes which may reveal sensitive information.

⇒ Remote Access Trojan: A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program such as a game or sent as an email attachment.

⇒ Distributed Denial of Service (DDoS) Attack Trojan: The goal of a DDoS Trojan is to cut off users from a server or network resource by overwhelming it with requests for service. While a simple denial of service involves one "attack" computer and one victim, distributed denials of service rely on armies of infected or "bot" computers able to carry out tasks simultaneously.

Be observant every time how your PC is behaving

Pinku: So mostly a Trojan is used for backdoor entry to seek information from one or more computer to take remote access control. OK... you used some term called Bot's above and what is that Dadaji?

Dadaji: A bot (short for "robot") is an internet robot an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input. There are many different types of bots, but some common examples include web crawlers, chat room bots, and malicious bots.

Spyware gathers your personal information

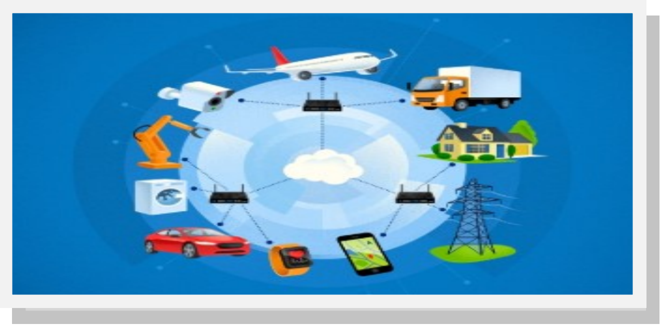
Pinku: Are there any good and bad bots Dadaji?

Dadaji: I wouldn't say a bot is a good or bad bot I only want to say this depends on how you use them. Good bots are beneficial to all online businesses. They help in creating the required visibility of the websites on the internet. When you search for a website or phrases related to the website's products or services, you get relevant results listed on the search page. This is made possible with the help of search engine spiders/bots, or crawler bots. In short, Pinku good bots are regulated. Bad bots, generally, don't play by the rules. They have a definitive 'malicious' pattern and are mostly unregulated. They can be sent by third-party scrapers or your competitors to steal content from your website.

Pinku: Can you give examples of sites which use bots?

Dadaji: Well! Facebook uses bots to grab the headline, first paragraph, and image from a story when you share it on your news feed. Meanwhile, Google uses bots to crawl and catalog the web so when you run a search, the site can deliver appropriate results.

Pinku: Hmm...who are mostly hit by bad bots Dadaji?



Computers were born to solve problems

Dadaji: Hackers use bots for all sorts of nefarious reasons, from lifting credit card numbers from an online store to scraping the text off an article and posting it on some random blog. Digital publishers, Travel sites, online stores, and real estate pages get hit hardest by bad bots.

Pinku: That was interesting insight you gave Dadaji. It's time now to discuss on Spywares. Tell me Dadaji what are they?

Dadaji: Spyware infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is mainly designed to gain access of your computer for the purpose of spying, often without your knowledge. Spyware gathers your personal information and relays it to advertisers, data firms, or external users. Usually it aims to track and sell your internet usage data, capture your credit card or bank account information, or steal your personal identity.

Nagware Nag's you

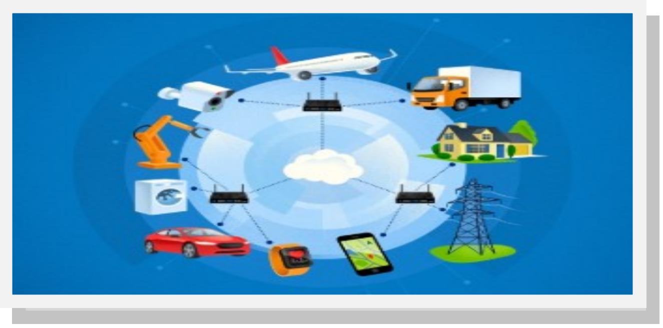
Spyware also monitors your login and password information, and spying on your sensitive information. Spyware is used for organizational purposes also for stealing data such as business plan, tender information and other such sensitive information.

Pinku: How does Spyware spy?

Dadaji: Spyware can use key loggers to obtain personal details such as the user's name, address, passwords, bank and credit information, and social security information. It can scan files onto the system's hard drive, watch other applications, install additional spyware, read cookies and modify the system's internet settings.

Pinku: That was useful information Dadaji. Now let's understand what a Nagware is?

Dadaji: As the name, Pinku its purpose is to nag or pester or annoy you time and again. Nagware is a software utility that "nags" users into upgrading or buying a premium version of software by sending constant pop-up messages or notifications. Software developers use Nagware as a marketing tactic to remind users to take advantage of special offers and purchase software. Nagware also call the user concentration on a specific content of a software program. For example, when a license of a program is expired, Nagware automatically and continuously shows a pop up to remind you for renewing the service. Nagware is also used in blog or news websites where you will see webmasters use it for extending the email listing.



Good Computer codes written do good to society

Pinku: Hmm... got it Dadaji. Now let's talk about Ransomware. Seems an interesting topic...

Dadaji: Yes Ransomware is very interesting topic indeed Pinku. As the name suggests, Ransomware is malicious software designed to block access to a computer system until a sum of money is paid.

Did you hear about "WannaCry"? Spread to more than 150 countries in a worldwide Ransomware outbreak which was the biggest cyber-attack. This malware encrypted data on infected computers and demanded a ransom roughly equivalent to £230 ($300).

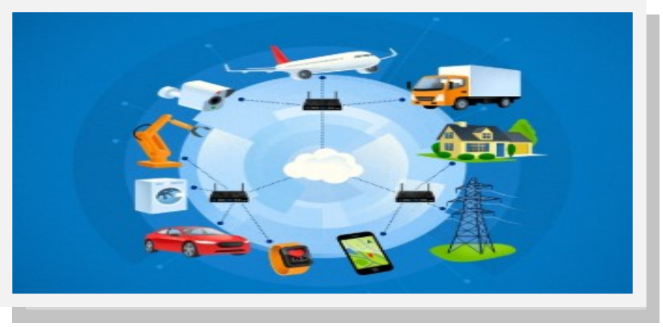
Adware is advertising-supported software

Pinku: WannaCry seems to be interesting tell me more Dadaji.

Dadaji: The attack was spread by various methods including phishing emails and on systems without up-to-date security patches. It mainly affected the National Health Service in UK. In detail, WannaCry was a Ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, and then demands a ransom payment in bitcoin (which is a form of alternate currency) in order to decrypt them.

Pinku: Hmm… my my… why people do such things Dadaji? Lest, lest discuss our next topic which is Adware…

Dadaji: Adware is the name given to programs that are designed to display advertisements on your computer, redirect your search requests to advertising websites and collect marketing type data about you for example, the types of websites that you visit so that customised adverts can be displayed. Adware that collects data with your consent should not be confused with spyware programs that collect information, without your permission. If Adware does not notify you that it is gathering information, it is regarded as malicious then.



Simple electronics make powerful computers

Pinku: How adware can be used for negative purposes Dadaji?

Dadaji: Well! a visit to an infected website can result in unauthorized installation of Adware on your machine. Hacker technologies are often used. For instance, your computer can be penetrated via browser vulnerability, and Trojans that are designed for stealthy installation can be used. Adware programs that work in this way are often called Browser Hijackers.

Pinku: Hmm… so you are asking me to be cautious Dadaji and not to visit sites which are not of any use to me.

Dadaji: Exactly Pinku. There are alluring sites which can be of great harm to you.

Pinku: Ok! Let’s move on to our next topic Dadaji what is a Shareware?

Shareware is distributed free on a trial basis

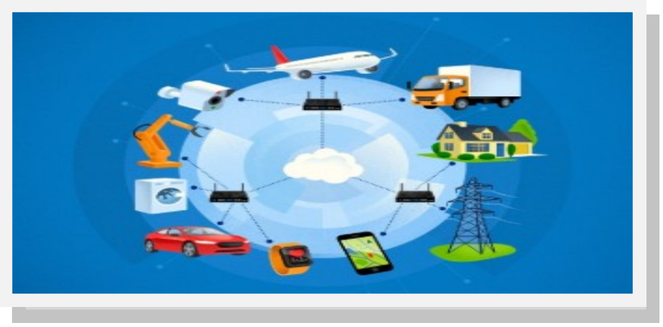
Dadaji: Shareware is software that is distributed free on a trial basis with the understanding that the user may need or want to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date. Shareware is also popular with gamers, as it gives them a chance to try a new game on a limited basis before purchasing the full version. It is also called as Demoware or trial software.

Pinku: Is Shareware harmful Dadaji.

Dadaji: Well Shareware is not harmful because usually they are copyrighted and are issued for commercial purpose. However, if the intent of individuals or companies who deliver shareware is bad, they can send malware in any form, (such as virus/worm/spyware) for malicious purpose into your computer.

Pinku: Hmm... makes sense. Ok, Dadaji now tell me what is a freeware then?

Dadaji: Well! Freeware is software that is available for use at no monetary cost. In other words, while freeware may be used without payment it is most often proprietary software, and usually modification, re-distribution or reverse-engineering without the author's permission is prohibited.



“The computer is down” is the most feared scenario

Pinku: Then what is the difference between shareware and freeware?

Dadaji: You already know the difference. The freeware is free for life and shareware is free only for the trial period.

Pinku: Ha! How harmful is then freeware?

Dadaji: Well! Similar to Shareware, Freeware also usually are copyrighted which is made available for use free. Let us see some of the features of freeware which can be harmful too:

- Freeware’s might be malwares as well. You never know.
- When the software is freely available, often developers will use advertising banners placed in the software which can nag you.

Pinku: Hmm...What might be the cons for using freeware then Dadaji?

Spams are always irrelevant to you

Dadaji: Let us see some of the cons:

⇒ Unfortunately most free or open source software is provided without support. This means that if you have a problem with the software the developer might or might not feel like helping you with that problem.

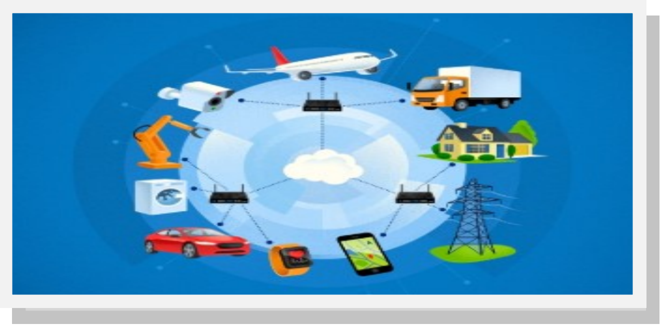
⇒ Some awesome geeks come up with fantastic software but they often lose interest or simply have no time to update or develop the software further.

⇒ Most developers that provide open source or free software don't waste time on the user interface. That means that the software might not look too fancy, in fact it will be plain and simple.

Pinku: Lest, if they are really useful, the cons are still OK at least they are available free… J…Let us get ahead Dadaji with our next topic what is a spam?

Dadaji: Spams are irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. If you observe, most of the emails such as yahoo come with spam filters/folders for better mail reading experience.

Pinku: What are the effects of spam Dadaji?



Computers are susceptible to deceases called the viruses, Trojans etc.

Dadaji: Here are some of the effects of Spam:

⇒ Wading through spam to find the legitimate email takes time, especially if you get a lot of them.

⇒ Reduces your Internet speed to a great extent.

⇒ Steals useful information like details on you Contact list.

⇒ Alters your search results on any search engine.

⇒ For a business owner, spam wastes workers' time and productivity and increases expenses because it consumes helpdesk and IT resources to deal with it.

⇒ Some spam carries email attachments that if opened can infect your computer with viruses or spyware. Spam can also be used to mass mail 419 scams or phishing emails.

Crippleware is half software

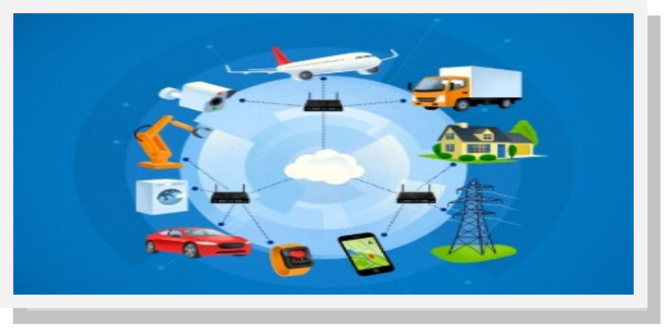
Pinku: What are these mass mail 419 scams Dadaji? Seems interesting…

Dadaji: Well! Pinku greed is something which is not at all good for any human. Nigerian scammers once took advantage of greedy one's with their tricky mass mails. The Nigerian scammers used to send mass emails to fraud people who were greedy and fall victim to their tricks. These were also called advanced fee scams, where a mail recipient is lured with huge money such as inheritance, or awards or lottery by paying advance money to receive the honors. The mailers would flee with your advanced money paid leaving you nothing. The name 419 refers to Nigerian criminal code for fraud.

Pinku: Ah! I Understood Dadaji. I always knew this that nothing comes free. If we put in our efforts and earn money, such money would stay with us long isn't it Dadaji.

Dadaji: Absolutely PinkuJ. Also, don't fall prey where people will lure you and ultimately you lose your hard earned money.

Pinku: Yes Dadaji I will always remember this. Now let's discuss our next topic which is Crippleware.



Computers does not understand civilizations but codes

Dadaji: To make you understanding easy i would define Crippleware as a crippled/ deliberately limited version of the full software package or hardware device. Crippleware is any software program that cannot be fully utilized until the user registers or, in the case of Shareware, purchases the program. To make it more simple, in Crippleware, functionalities such as printing or the ability to save files are disabled. There is a similar business model used in IT industry termed as Freemium. A small difference I assume is Crippleware will omit or restrict features that are needed for basic operations in the application whereas, Freemium tempts users to pay who like the basics model but "want more" or need advanced versions of this feature.

Pinku: So what's wrong with Crippleware or Freemium's?

Dadaji: Once again Crippleware and Freemium since they are free, versions of these

Postcardware comes with licensing agreement

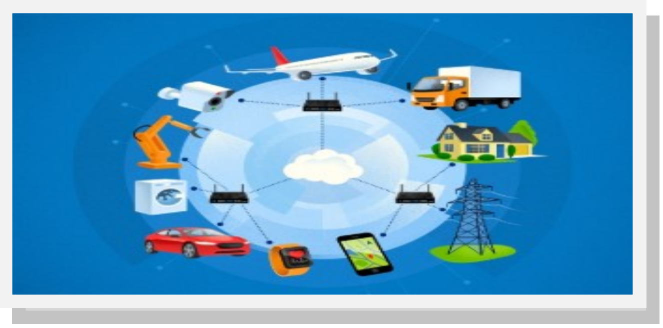
software programs can have possible mix of spyware or worms in it. Hence, read a bit of background of the companies which issue Crippleware or Freemium's.

Pinku: Hmm... Ok! Let's now talk about Donationware...

Dadaji: Donationware is software that is free to use, but encourages users to make a donation to the developer/some cause. Donationware is put out in the spirit that if you use it regularly, you should make a donation.

Pinku: Since it is free there can be viruses, spywares or worms in it right Dadaji?

Dadaji: Could be... not all Donationware have it. Now let me finish explaining you the last ware that I am aware about called Postcardware. It is also called just Cardware, is software similar to shareware, distributed by the developer on the condition that users send the developer a postcard. Basically, the developer enjoy receiving postcards from all over the world and think it's a nice way for users to show appreciation without becoming poor sending a postcard is cheap anywhere in the world. It's again a type of freeware so I need not have to explain you what's wrong.



Computers cannot dream for you

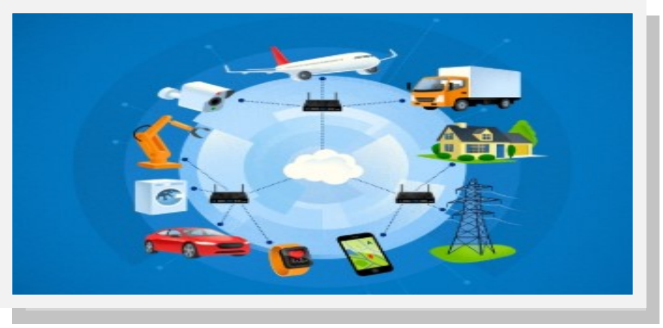
Pinku: You exquisitely explained the basics Dadaji. Now, I want to listen more stories and if you could also give scenarios of computer frauds.

Dadaji: Oh! Sure Pinku. Let me start with story of Melissa Virus; it was a macro virus that was distributed as an e-mail attachment. When opened, it disabled a number of safeguards in Word 97 or Word 2000, and, if the user had the Microsoft Outlook e-mail program, caused the virus to be resent to the first 50 people in each of the user's address books. Melissa arrives in an attachment to an e-mail note with the subject line "Important Message from the name of someone [," and body text that reads "Here is that document you asked for...don't show anyone else ;-)". The attachment is often named LIST.DOC. If the recipient clicks on or otherwise opens the attachment, the infecting file is read to computer storage.

I Love you virus was a worm

Pinku: That was interesting… tell me more Dadaji…

Dadaji: Similar to Melissa, “Iloveyou” virus was created even though those who written it denied that they were not even aware of Melissa. The Iloveyou virus also known as the love letter virus was actually a computer worm originating in the Philippines. The worm was reported to have come from a couple of the ages 23 and 27 after a raid of their Apartment in Philippines. The virus arrived in an email with the subject line of "ILOVEYOU" with an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs" that people were encouraged to open, since the ".vbs" suffix was not visible, thus seeing the ".TXT" suffix. The message body is "kindly check the attached Love letter coming from me." Love letter searches for files to modify, mostly by replacing those files with a copy of itself. If the file has a .vbs or .vbe extension, it will simply overwrite the files. If they have the extensions js, jse, css, wsh, sct, or hta, it will overwrite the file as well as the extension, changing it to .vbs, but retaining the original name (program.js becomes program.vbs). For .jpg or .jpeg files, it overwrites them, retains the original file name and extension, but adds .vbs to the extension (picture.jpg becomes picture.jpg.vbs). Mp3 and mp2 files are not overwritten, but rather hidden. Love letter opens the Outlook email program and scans for email addresses in the Address book. It sends the email with an attached copy of itself. This is what Melissa did. The virus has caused companies, governments, and end-users extreme grief shutting down mail systems, mail servers, and bank systems.



Your brain is the biggest computer identified

Pinku: Hmm… what’s the next story Dadaji?

Dadaji: Well next I am going to tell you about a worm by name Code Red. Code Red was a computer worm observed on the Internet in 2001. It attacked computers running Microsoft's IIS web server. The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permeh. They named it "Code Red" because Code Red Mountain Dew was what they were drinking at the time.

Nimda was actually opp. of Admin

Code red exploited an operating system vulnerability that was found in machines running Windows 2000 and Windows NT. The vulnerability was a buffer overflow problem, which means when a machine running on these operating systems receives more information than its buffers can handle; it starts to overwrite adjacent memory. Code red not only disrupted around 300000 computers but also tried DDoS (Distributed denial of service) attack on the whitehouse.gov site.

Pinku: Oh my god! Why people write such programmed viruses and worms Dadaji?

Dadaji: Well! They are usually written to exploit someone for something. Oh I forgot to tell you that after Code Red came another worm named Code Red II causing possible billions of dollars of damage in the summer of 2001. It is also one of the few worms able to run entirely in memory, leaving no files on the hard drive or any other permanent storage.

Pinku: Was this worm detectable Dadaji?

Dadaji: Well! That was the biggest problem with this worm. It was not easily detectable. Also, I forgot to mention Pinku that this worm required around 2 billion USD to clean up.

A Computer programming comes with bugs as a package

Pinku: Ok! Let's move on Dadaji what is our next virus/worm/Trojan that caused havoc/ losses…

Dadaji: Let us know talk about Nimda Virus. Another virus to hit the Internet in 2001 was the Nimda (which is admin spelled backwards) worm. Nimda spread through the Internet rapidly, becoming the fastest propagating computer virus at that time. In fact, it only took 22 minutes from the moment Nimda hit the Internet to reach the top of the list of reported attacks. The Nimda worm created a backdoor into the victim's operating system and took control of victim's computer. Rather i would say Nimda now also become the admin (/users) of the computer it attacked. The virus caused $635 million worth of damages in 2001 and caused Internet browsing time to slow significantly.

Pinku: Why do people release such viruses?

SQL Slammer caused a denial of service

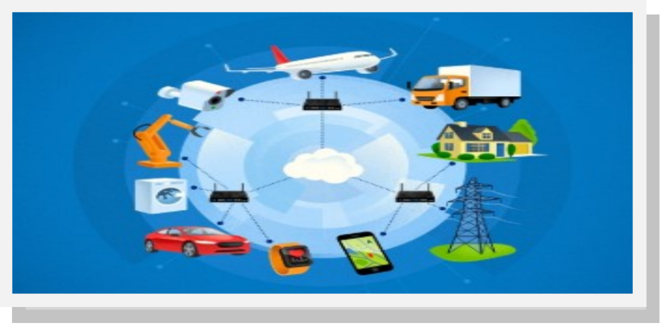
Dadaji: There are hundreds of thousands of viruses out there and they often are designed for different objectives such as

- To take remote control of victims computer and use it for specific tasks
- To get ransom
- To theft personal data or sensitive information (Tender information, business plans, Commercial card details (credit/debit cards), passwords…)
- To prove a point, to prove it can be done, to prove ones skill
- To cripple a computer or network
- To take revenge
- To protect one's own business (as you now know the example of Basit and Amjad's "Brain")

Pinku: You summarized it all Dadaji…Let us get ahead Dadaji.

Dadaji: Let me now talk about "SQL Slammer" spread in the year 2003. It spreads by scanning the Internet for vulnerable systems, and it is this scanning activity that has degraded service across the entire Internet. Taking 15 minutes to spread worldwide, the SQL Slammer worm was one of the largest and fastest spreading worms ever. For this reason, some have described Slammer as the first "Warhol worm" (had its 15 minutes of fame). The virus was infected around 350,000 computers. Some of the major damages it has done:

- In the United States, Windows XP activation servers in Redmond, Washington were taken offline.
- Continental Airlines resorted to pens and paper to record reservations and tickets. The airline had to delay and cancel some flights, though no delays lasted more than 30 minutes.
- A majority of Bank of America's ATMs were rendered as useless for the whole day. Washington Mutual's ATMs and other bank services were unavailable for most of the day.



Secure your computers with strong passwords

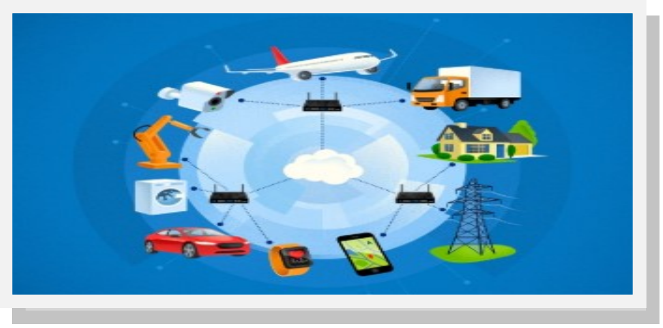
Lovsan is a network worm

- Customers of the Canadian Imperial Bank of Commerce in Toronto were unable to withdraw money using ATMs.
- The U.S. departments of State, Agriculture, Commerce and Defense were infected with the worm.
- The Emergency 911 network was down for some time.
- South Korea was particularly hit hard by the worm. The Korean media claimed that the entire Internet infrastructure was knocked out. Customers of the ISP KT Freetel Corp and SK Telecom lost their internet connections.
- In Portugal, more than 300,000 customers of Cable ISP Netcabo lost internet access.

Pinku: Oh! My my so much of damage... Tell me more Dadaji.

Do not fall for offers that you don't know or don't understand

Dadaji: Well now it's time to talk about Blaster, also known as Lovsan or LoveSan 3a1. This worm came from United States on August 11, 2003, and only affected computers with operating systems that had Windows 2003/XP/2000/NT. Blaster was a worm which exploited vulnerability in Windows 2000, Windows XP, and Windows NT systems to propagate itself by spreading and executing a file named Msblast.exe on infected systems. The Blast worm was programmed to coordinate infected systems in launching a denial of service attack against the web site windowsupdate.com. Microsoft Security Bulletin MS03-026 explains the Windows vulnerability exploited by the Blaster worm and provides patches for affected systems. Blaster contained the message in your code: "I just want to say I love you San!" (We still do not know who San is) and added, "Billy Gates, why do you make this possible? Stop making money and fix your software. 2 Billion Computers had been infected with a self-replicating worm known as Blaster. .



Pinku: I think I understood most of the worms/Trojans/viruses. Let's discuss something new Dadaji, may be about frauds in computer.

Dadaji: Oh! Sure Pinku...! Do you know what Phishing is?

Phishing is attack more

Pinku: Oh Yes Dadaji, my computer teacher taught me this. Phishing dupes a victim into opening an email, instant message, or text message that either has a “malware” or a “lure” which makes victim lose money.

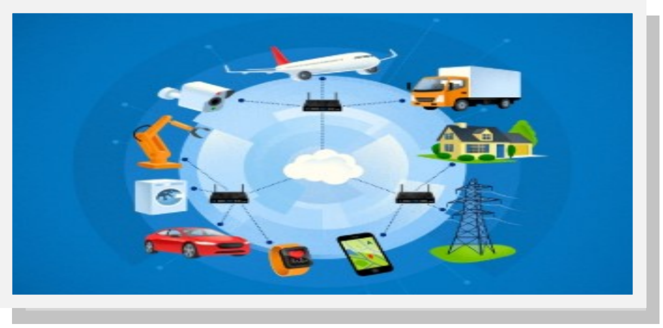
Dadaji: That’s great… you know it all. Do you know Pinku that phishing is a numbers game. An attacker sends out thousands of fraudulent messages but, only expect a small percentage of recipients fall for the scam. There are several techniques attackers use to increase their success rates. For example, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization, using the same phrasing, typefaces, logos, and signatures which make the message appear legitimate. Let me show you an example of a phishing mail:

My School

To me,

Subject: Important! Your password will expire in 1 day.

Dear Network user,



Let your computer block the pop ups as they are most likely loaded with viruses

This mail is meant to inform you that your School network password will expire in 24 hours. Please follow the link below to update your password.

www.Pwdrenewalschoolname.com/renewal

Thank you

School Name (with Logo)

Here two things can happen if you open the link

⇒ When you supply your original username and password, the hacker can use this information to get into your school network using your password.

⇒ A malicious script activates in the background to hijack school network.

Phishing is attack more

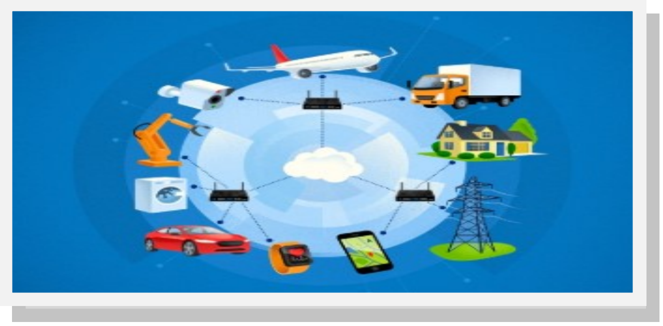
You have to observe two important things in the above mail; one attacker will usually try to push users into action by creating a sense of urgency and two, threaten that the account will expire soon. Applying such pressure causes the user to be less diligent and more prone to error. If you are observant Pinku, you will see that the links inside messages will resemble legitimate counterparts, but typically have a misspelled domain name or extra subdomains. In the above example, the www.Pwdrenewalschoolname.edu/renewal

URL was changed to www.Pwdrenewalschoolname.com/renewal.

Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place. Usually schools and educational websites end with .edu meaning education and.com meaning company. Similarly Pinku, you should also know that official government websites end with .gov, .org means organizations so and so forth.

Pinku: Ah! So much of fraud... Tell me more Dadaji.

Dadaji: Did you hear the term Vishing?



Do not fall victim for lucrative offers you receive through mails

Pinku: No Dadaji... but it must be similar to Phishing.

Dadaji: Absolutely. The term Vishing comes from voice or voip Phishing. A Vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. Vishing is fraudulent practice of making phone calls or leaving voice messages claiming to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers and fraud the victim.

Pinku: Oh! So I should be careful with my telephone as well...

Dadaji: Yes Pinku you should be. Let me now tell you what a information warfare is all about. Gathering of information to distort somebody or somebodies plans by doing alterations via communication infrastructure, composed of networks of computers, routers, telephone lines, fiber optic cable, telephones, televisions, radios, and other data transport technologies and protocols.

Denials of Service can numb a country

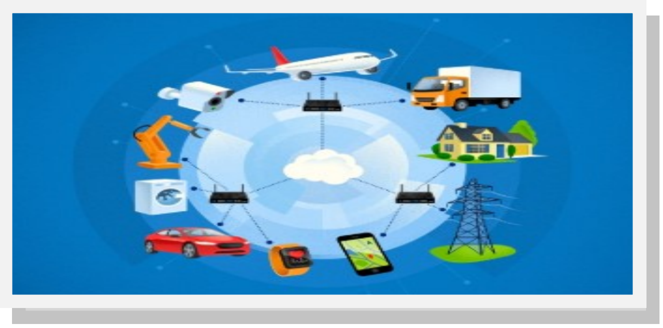
There are three techniques of Information warfare namely, disturbance, degradation, and denial of services.

Pinku: Ah! Interesting… So now countries do not have to go for war. Quash one's information or activate denial of internet related services will numb the whole country.

Dadaji: Exactly! Some of the more popular weapons used to wage these types of information warfare are spoofing, noise introduction, jamming, and overloading. This is what is going to be the next generation's type of war "the information warfare". You know through information one could win even win elections by campaigning for the topic (/s) what majority of mass population's thinks is appropriate.

Pinku: Very interesting. So you mean to say information is god…

Dadaji: Yes in the modern age that is true. Let me now tell you about spoofing. The word "spoof" means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.



Do not share your IP address to anyone whom you do not know

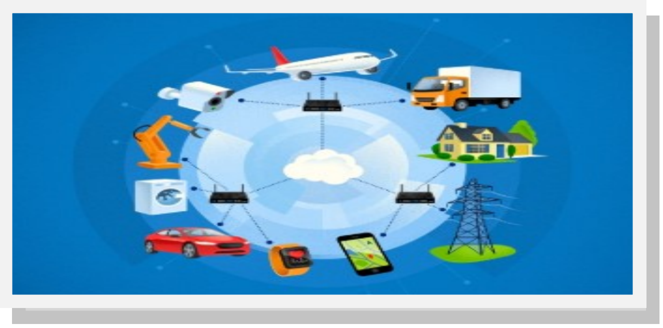
Spoofing can take place on the Internet in several different ways. One common method is through e-mail. E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message. Another way spoofing takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server.

Skimming is a compromise technique

Pinku: Spoofing such a funny name Dadaji isn't it?

Dadaji: Yes! But if you are victim of spoofing than that is not at all funny Pinku. Let me now tell you about skimming. Skimmer is the name of the person who participates in skimming frauds. Skimmer illegally collects data from the magnetic stripe of a credit or debit card. When you try to swipe through skimming machines, your card information is copied onto another blank card's magnetic stripe, which is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder. Skimming also works by replacing a card reader like an ATM with a camouflaged counterfeit card reader. The counterfeit reader records all of the data on a credit, debit or ATM card as it passes through the skimmer. In addition to ATMs, other locations where card skimming happens include restaurants, taxis or other businesses where an employee will take the card from the actual account holder in order to run the charge. In these instances, the thief has fitted the card reader with a skimmer device, or uses a hand-held skimmer device hidden in a pocket.

Pinku: What are you talking Dadaji, even ATM centers and restaurants are also not safe. Oh! Pretty... Well Dadaji aren't they hackers then?



Hackers are clever, don't give them chance to show their cleverness

Dadaji: Oh Yes, they are. Do you know Pinku, Hacker while this term originally referred to a clever or expert programmer; it is now more commonly used to refer to someone who can gain unauthorized access to other computers. A hacker can "hack" his or her way through the security levels of a computer system or network.

Pinku: Ah! That is a more sensible definition. Tell me more Dadaji...

Dadaji: Oh sure Pinku. Do you know there are several types of hackers?

Pinku: Is it?

Dadaji: Yes Pinku and her you go:

1. White Hat Hackers: The term "white hat" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies that ensures the security of an organization's information systems are secure.

Hackers wear different hats

In two seconds your phone can be hacked. Do not give your phone to strangers

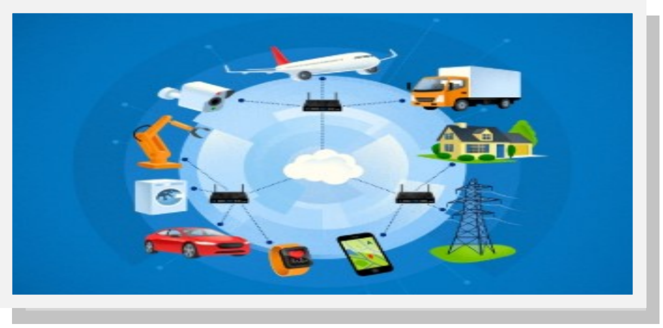
- ⇒ Black Hat Hackers: Black hat hackers are the classic definition of a real hacker an aggressive computer user who willfully breaks into, vandalizes or commits theft on other peoples' networks. 'Black hat' is simply the way we refer to their malicious motivations. They are often motivated by greed or revenge, and that fuels their desire to break into other peoples' networks and wreak havoc.
- ⇒ Red Hat Hackers: Red Hat Hackers are hunters of black hat hackers. They are ruthless when it comes to dealing with black hat hackers meaning, instead of reporting a malicious attack, they take on the black hat hacker completely by launching a series of aggressive cyber-attacks and malware on the black hat hacker that they may as well have to replace the whole system or shut down.
- ⇒ Gray Hat Hackers: Gray hat hackers fall somewhere in between white hat and black hat hackers. Because a gray hat hacker doesn't use his skills for personal gain, he is not a black hat hacker. Also, because he is not legally authorized to hack the organization's cyber security, he can't be considered a white hat either.
- ⇒ Hacktivists: They can be social/political/religious activists who do a socio/political/religious propaganda. Hacktivists is a hacker or a group of anonymous hackers who think they can bring about changes.
- ⇒ Script Kiddies: A term often used by amateur hackers who don't care much about the coding skills. These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is often to impress their friends or gain attention.
- ⇒ Green Hat Hackers: These hackers are the amateurs in the online world of hacking. Consider them script kiddies but with a difference that these newbies have a desire to become full-blown hackers.

- ⇒ And. are very curious to learn. You may find them engrossed in the hacking communities bombarding their fellow hackers with questions.
- ⇒ Blue Hat Hackers: These are another form of novice hackers much like script kiddies whose main agenda is to take revenge on anyone who makes them angry. They have no desire for learning and may use simple cyber-attacks like flooding your IP with overloaded packets which will result in DoS attacks. A script kiddie with a vengeful agenda can be considered a blue hat hacker.

That reminds me of tech support scams. Did you hear about it?

Pinku: No Dadaji and what's that?

Dadaji: Scammers call and claim to be computer techies associated with well-known companies or send pop-up messages that warn about computer problems. They say they've detected viruses or other malware on your computer. They claim to be "tech support" and will ask you to give them remote access to your computer. As soon as you give remote access to them, they can steal all the data from your computer. Some scammers will diagnose a non-existent problem and ask you to pay for the services. So the learning for you Pinku is if you get an unexpected pop-up, call, spam email or other urgent message about problems with your computer, "Stop", don't click on any links, don't give control of your computer and don't send any money.



Be careful while giving remote access to strangers

Pinku: Oh gosh! Dadaji this is crazy… Whom to believe and whom not to?

Dadaji: It's simple Pinku. Always note down the numbers of authorized service givers of the brand of computer you are using.

Pinku: Makes sense. Tell me more Dadaji.

- ⇒ Dadaji: I will teach you a new term Hacktivism. Hacktivism is use of computers and computer networks to promote a political or social agenda. Hacktivism is a mix of "hacking" and "activism". The meaning of the term was loose and could span passive actions, such as just expressing an idea,

Eavesdropping is listening to private conversation

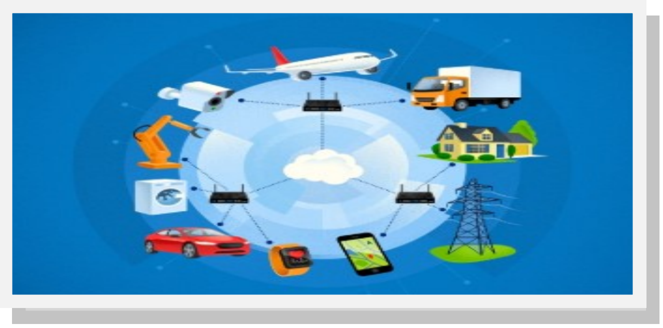
to malicious attacks targeting ideological opponents. Hacktivism, as a term, has become more prevalent in recent years and describes groups or individuals who plan to affect political change or ideological change. The people who believe in Hacktivism are called hacktivists. Unlike cyber criminals who hack into computer networks to steal data for the cash, most hacktivists aren't doing it for the dollars. They're individuals or groups of hackers who band together and see themselves as fighting injustice.

Pinku: Hmm… so activists are doing protests using computers as well… I do not know where the world is moving?

Dadaji: True but that's how it is. Now let us understand Cyberterrorism. It is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence. Unlike a virus or computer attack that results in a denial of service (DoS), the cyberterrorist attack as explicitly designed to cause physical harm to individuals. Cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers and water systems.

Some malicious software are comingled with genuine software. Beware!

Pinku: Oh God! So many activities are happening in this world.



Dadaji: Yes Pinku. We should be even aware of networks which are not secured. Let me tell you about eavesdropping. An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

Pinku: Ah! So this may include IP phones and smart phones via network.

Dadaji: Yes, Absolutely… Public Wi-Fi networks are an easy target for eavesdropping attacks.

Man in the middle is a super actor

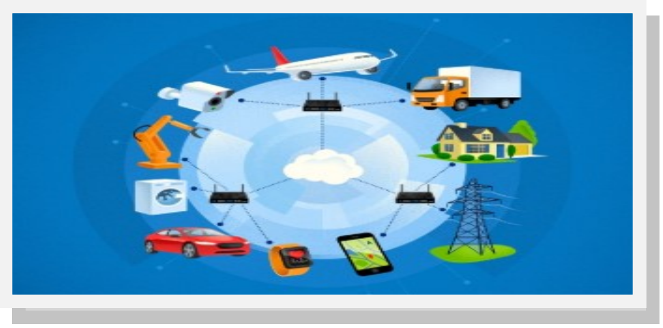
Anyone with the easily available password can join the network and use free software to monitor network activity and steal login credentials and valuable data that users transmit over the network. This is one way people get their Facebook and email accounts hacked.

Pinku: Oh my God! I have to inform my father he usually asks for wifi connections in coffee shops and pastry shops.

Dadaji: Similar to eavesdropping, there is another concept called “A man-in-the-middle (MITM)” attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.

Pinku: Ah! How mean Dadaji… Tell me more about such attacks.

Dadaji: Let me now tell you about sniffer attack. A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. A sniffer provides a full view of the data inside the packet. Using a sniffer, an attacker can read your communications and by analyzing your network, can gain information to cause your network to crash and become corrupted.



Don’t panic on Ransomware attack

Pinku: Oh! So, sniffers even give chance to people who are not tech savvy.

Dadaji: Yes Pinku absolutely. Continuing let me tell you about application-layer attack. An application-layer attack targets application servers by causing a fault in a server’s operating system or applications. The attacker gains the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do the following:

⇒ Read, add, delete, or modify your data or operating system.

- Introduce a sniffer program that analyzes your network and gains information that can be used to crash or to corrupt your network and systems.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Disable other security controls to enable future attacks.
- Abnormally terminate your operating systems and data applications.

Do you know these attacks are called cyber-attacks? If i were to define it, it is offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

Pinku: Hmm... cyber-attacks. Wow! That seems to be a good terminology. I heard a terminology called Cyberstalking and what is that Dadaji?

Dadaji: Cyberstalking is the use of the Internet or other electronic means to stalk someone. It has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, the transmission of threats, identity theft, and damage to data or equipment for harassment purposes.

Cloud computing is better alternative for traditional hosting servers

Pinku: Ah! So it has similar meaning of stalking. I think we should stop it here Dadaji, it’s time for me to go to school.

Dadaji: Yes absolutely...OK Pinku, it’s time for me to go for a walk.

Pinku: Oh sure carry on Dadaji. I will remember today’s Gyan (knowledge) given by you. See you in the evening as by the team you come from walking, I would have gone to school.

Computer is a boon if you use it optimally But, becomes a bane when overused or for malicious purposes

Thank You