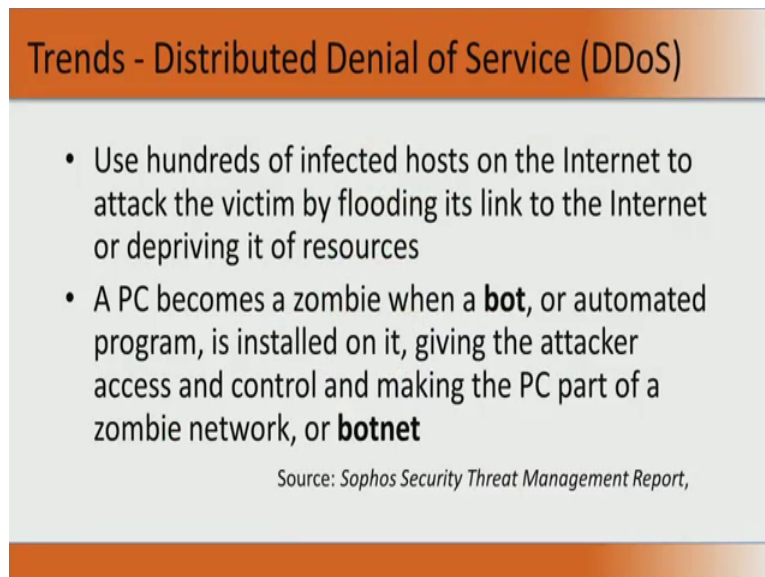


Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 20

We now talk about distributed denial of service which is another trend of attacking your PC. Now, a PC is connected to the internet, but then it cannot access the internet because the link between the PC to the internet is being clogged by hundreds of other infected force on the internet and they will be flooding it with traffic, so that your being switched resource, right your PC actually gets very less time to connect and download data. Now, this type of flooding the network with spurious packets or useless packets is called a denial of service and since this is happening from host distributed across the internet, it is also called a distributed denial of service. DDOS has become very increasingly big nuisance and so, what happens is actually a PC has a malware installed in it and that malware can start bot. As I told you a bot is something that is software that can run automated scripts on the network.

(Refer Slide Time: 01:56)



Trends - Distributed Denial of Service (DDoS)

- Use hundreds of infected hosts on the Internet to attack the victim by flooding its link to the Internet or depriving it of resources
- A PC becomes a zombie when a **bot**, or automated program, is installed on it, giving the attacker access and control and making the PC part of a zombie network, or **botnet**

Source: Sophos Security Threat Management Report,

So, then actually PC now becomes part of this bot net once it has this malware, and this malware gets installed without the user's knowledge because through a spyware or through a malware. This starts flooding the network with traffic and essentially it creates an availability issue for the system.

(Refer Slide Time: 02:04)

Latest Trends - DDoS - continued

- Zotob Worm –
 - most high profile botnets of 2005
 - achieved worldwide notoriety in August
 - leading media organizations including ABC, The Financial Times, and The New York Times fell prey to it

So, some of the early DDoS attack was this Zotob worm, worm which came into 2005 and actually it achieved worldwide notoriety in August of that year and leading media organizations including ABC, The Financial Times, and New York Times actually fell prey to it. So, this was one early distributed denial of service attack. So, we now saw that there is a PC is very much responsible. A PC if it becomes a malware, if it has a malware which can spawn a bot, the PC itself is not just compromised, but entire network can get compromised.

(Refer Slide Time: 02:50)

Best Practices to Help Protect Your Digital Assets

- Anti-virus software
- Anti-spyware software
- Windows and applications updates
- Security bundles
- Personal firewalls
- Wireless Security
- Other best practices

The entire network can become unavailable, an entire network can suffer from this availability issue because one PC, there is bunch of PCs on are have become vulnerable

or have become inflicted. So, we have been repeatedly telling in the module 1 that people have to protect themselves, people need to be protected and what do you mean by a person been protected the system that is working on should be protected. So, how do you protect your PC? So, there are lots of things that come in. For example, antivirus software, anti spyware software, windows and application updates security bundles, personal firewall, wireless security, and other practices. Now, we are in this sort of a very bad state. We actually buy software and then, we actually buy software to secure that software sort of very disturbing state.

Why this has happened because over a period of time when PC since was invented, people never thought that this PC is going to be a part of million PCs internet. People never thought a PC can be shared if they would have called it as a SC or shared computer rather than a personal computer. When the PC came into existence and operating systems were written, they never had a clue that somebody can use the operating system weaknesses to go and attack. In still early times nobody assumed that the PC will become an asset. These were just use like calculator or a compute tool. PC can store very important confidential information. If your PC is lost; your carrier is lost. So, these types of things people never conceived. So, because of that security actually went into the back burner. So, security was always sold as an additional thing, and customers did start viewing as an additional financial burden rather than a real protection.

So, many of the conventional operating systems and software's were not written with security as a prime objective, and that is why when you buy these operating systems, you have to go and buy another set of software and hardware to go and secure this operating system. So, security is not part of the back bone of software development, not part of the implementations, software implementations, inside an organization and security being viewed separately from the software, security being decoupled from the operating system. These are some of the reasons why today we are in this state with respect to information security.

You will also understand that security needs to grow with the design. It cannot be suddenly added into a design. It starts from the day one when the design starts. So, security should be embedded in. These are some of the reasons why we still have issues in protecting our digital assets. So, these issues get solved by having some other software which will go and ensure protection, but still it is not part of the core software. We need to accept today that the core software running in a system and the applications that use a

set of core data inside this system are still vulnerable to attacks.

(Refer Slide Time: 07:01)

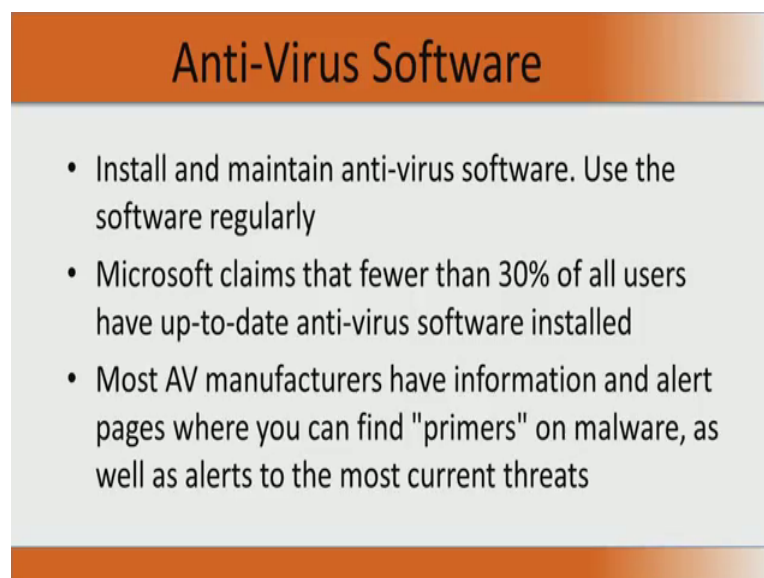


Best Practices to Help Protect Your Digital Assets

- Anti-virus software
- Anti-spyware software
- Windows and applications updates
- Security bundles
- Personal firewalls
- Wireless Security
- Other best practices

To address those vulnerabilities, we have listed seven best practices. What is a practice here? Go and buy the software and install them properly. Now, we have seen this. Now, we will see more about these best practices in this lecture in a little more detail.

(Refer Slide Time: 07:15)



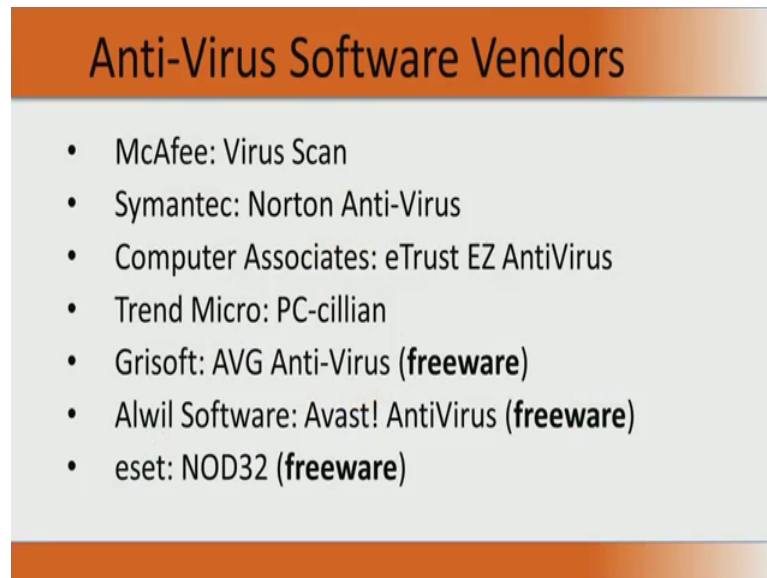
Anti-Virus Software

- Install and maintain anti-virus software. Use the software regularly
- Microsoft claims that fewer than 30% of all users have up-to-date anti-virus software installed
- Most AV manufacturers have information and alert pages where you can find "primers" on malware, as well as alerts to the most current threats

So, antivirus everybody use, but Microsoft actually claims based on their internal survey or survey they are conducted that fewer than 30 percent of all users have up to date antivirus software. If you do not have up to date antivirus software, you essentially have certain vulnerabilities that are not fixed and people can attack through those

vulnerabilities. Most of these antivirus manufactures have information and alert pages and where you can find primers on malware, education to malwares, as well as alerts to most current threats.

(Refer Slide Time: 08:08)



Anti-Virus Software Vendors

- McAfee: Virus Scan
- Symantec: Norton Anti-Virus
- Computer Associates: eTrust EZ AntiVirus
- Trend Micro: PC-cillian
- Grisoft: AVG Anti-Virus (**freeware**)
- Alwil Software: Avast! AntiVirus (**freeware**)
- eset: NOD32 (**freeware**)

So, this are the list of several antivirus softwares. Some of them are the Grisoft, Alwil Software and EZ are free. They are freeware.

(Refer Slide Time: 08:16)



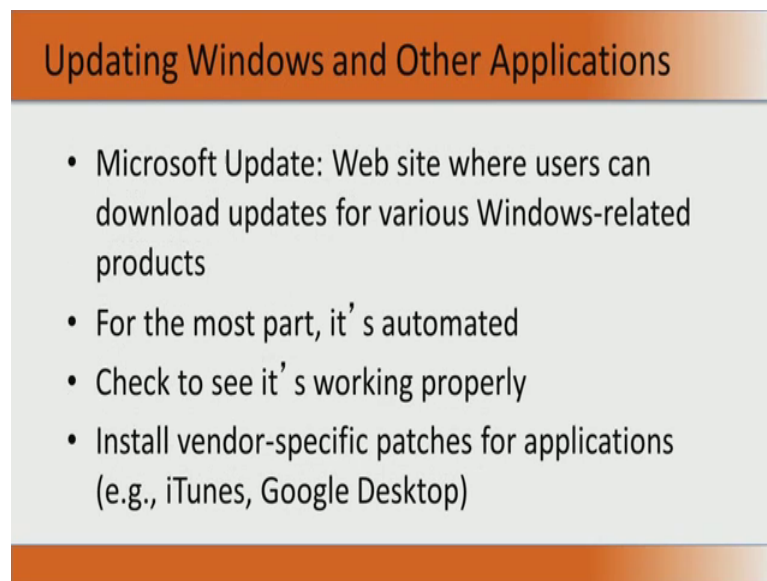
Anti-Spyware Software

- Install and maintain anti-spyware software
- Use the software regularly
- Sunbelt Software: CounterSpy
- Webroot Software: Spy Sweeper
- Trend Micro: Anti-Spyware
- HijackThis (**freeware**)
- Lavasoft: Ad-Aware SE Personal (**freeware**)
- Spybot: Search & Destroy (**freeware**)
- Microsoft: Windows Defender (**freeware**)

Then next thing is the anti-spyware software. So, this needs to be also installed and maintained and we need to use the software regularly and then, you see a lot of things Counter Spy, Spy Sweeper and Anti-Spyware, Hijack This, Ad-Aware SE Personal,

Search and Destroy, Windows Defender. Some of them are also freeware.

(Refer Slide Time: 08:49)



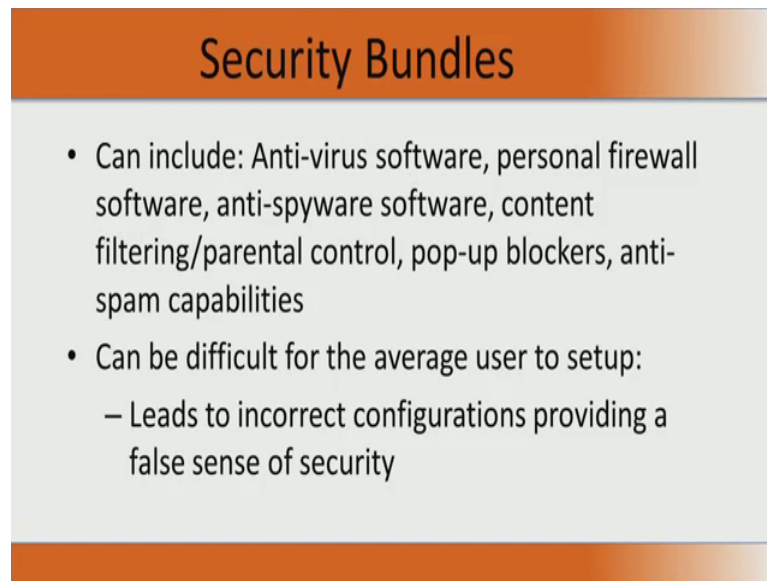
The slide features a title bar at the top with a gradient from dark orange to light orange. Below the title bar is a light gray rectangular area containing a bulleted list. At the bottom of the slide is another gradient bar, matching the top one.

Updating Windows and Other Applications

- Microsoft Update: Web site where users can download updates for various Windows-related products
- For the most part, it's automated
- Check to see it's working properly
- Install vendor-specific patches for applications (e.g., iTunes, Google Desktop)

Another important thing is that we need to keep updating our operating system like for example, update windows and all other applications and each update will have something to do with security. If you see some of the latest updates of say Microsoft or other organization, a significant part of it is to go and fix some vulnerability. For the most part of updating windows or micro soft operating system, it is automated. One can just go in and need not even click. It can be automated, but we can go and check whether the new patch is working properly. Similarly for every software, there is vendor specific patches and all these operating systems gives your quick way of going and updating all these patches.

(Refer Slide Time: 09:55)

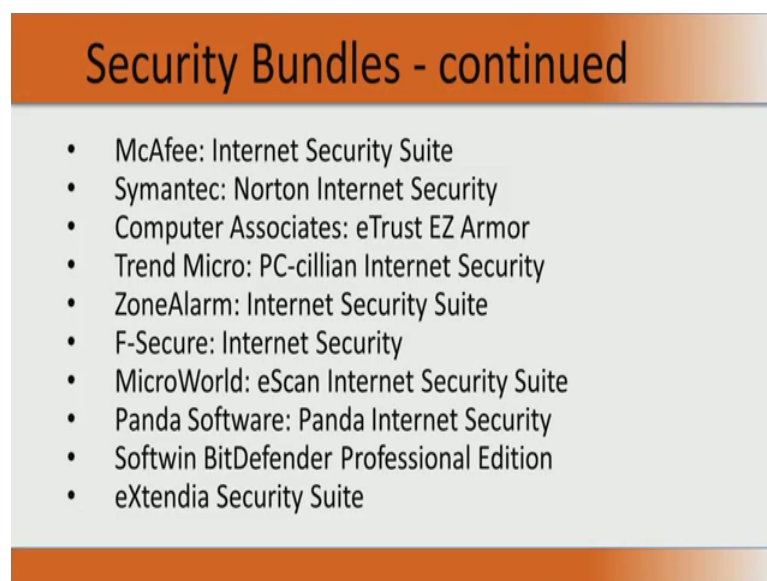


Security Bundles

- Can include: Anti-virus software, personal firewall software, anti-spyware software, content filtering/parental control, pop-up blockers, anti-spam capabilities
- Can be difficult for the average user to setup:
 - Leads to incorrect configurations providing a false sense of security

Now, we will see some commercially available, commercially off the shelf software that is available which can take care of this problem that we have posed here. So, the one of the things is security bundle which includes anti-virus, personal firewall, anti spy ware, content filtering, parental control, pop-up blockers, anti-spam capabilities, everything. The most important thing is when you have a security bundle; each of these would require some amount of knowledge to implement it and for an average user to use all these things could be very difficult because they may lead to incorrect configurations and once you have incorrect configuration, this will give you a false sense of security.

(Refer Slide Time: 10:58)



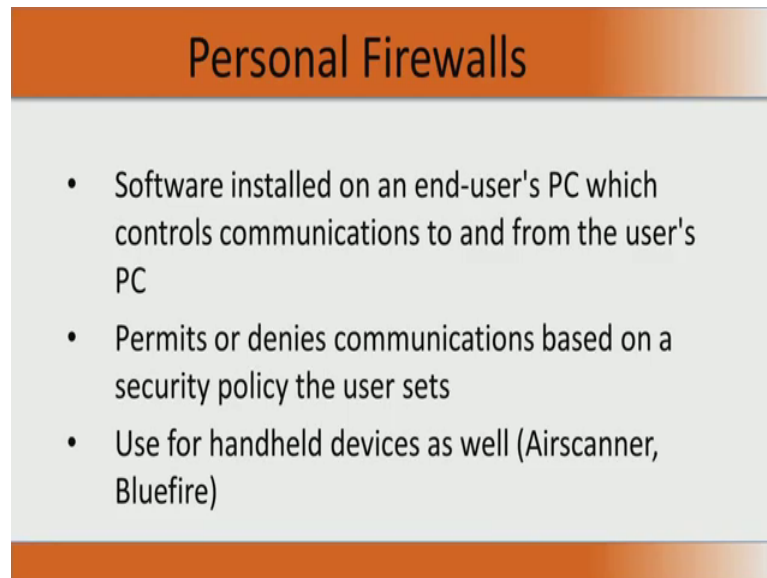
Security Bundles - continued

- McAfee: Internet Security Suite
- Symantec: Norton Internet Security
- Computer Associates: eTrust EZ Armor
- Trend Micro: PC-cillian Internet Security
- ZoneAlarm: Internet Security Suite
- F-Secure: Internet Security
- MicroWorld: eScan Internet Security Suite
- Panda Software: Panda Internet Security
- Softwin BitDefender Professional Edition
- eXtendia Security Suite

Many security bundles do exist of McAfee, Symantec, Computer Associates, Trend

Micro, Zone Alarm, F-Secure, Micro World, Panda Software, Softwin BitDefender Professional Edition, eXtendia Security Suite. So, many things exist as security bundles which can be used to get the desired level of security.

(Refer Slide Time: 11:28)



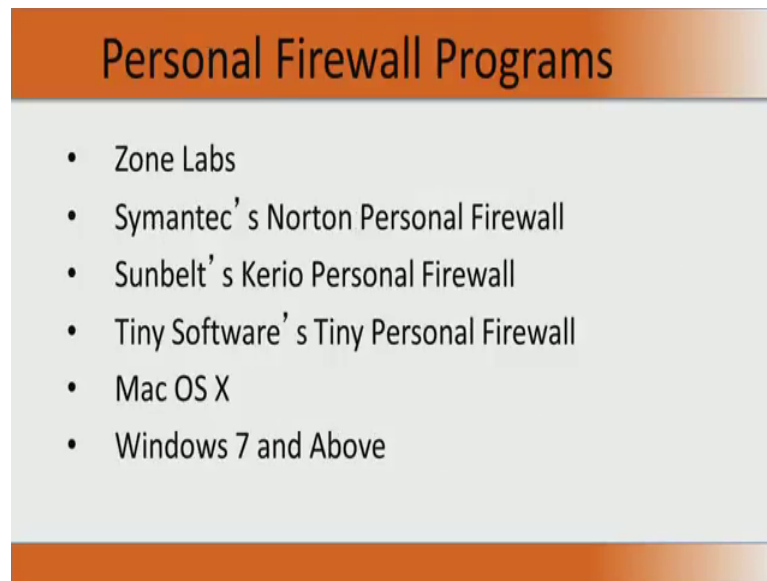
The slide features a title 'Personal Firewalls' in a dark orange header bar. Below the title, on a light gray background, are three bullet points. The slide is framed by orange bars at the top and bottom.

Personal Firewalls

- Software installed on an end-user's PC which controls communications to and from the user's PC
- Permits or denies communications based on a security policy the user sets
- Use for handheld devices as well (Airscanner, Bluefire)

Now, we talked about anti-virus and anti-spy ware and security bundles. Now, we will talk about how to protect the PC from the internet. So, every PC can be populated with a personal firewall. So, what will the personal firewall do? It will permit or deny communication based on security policy that you put on the system. These types of personal firewall should be extremely useful, specifically for hand devices, hand-held devices as well. So, you can go and Google on AirScanner and Bluefire. These are personal firewalls for the hand-held devices like your mobile phones.

(Refer Slide Time: 12:21)



Personal Firewall Programs

- Zone Labs
- Symantec's Norton Personal Firewall
- Sunbelt's Kerio Personal Firewall
- Tiny Software's Tiny Personal Firewall
- Mac OS X
- Windows 7 and Above

There are many personal firewall programs like Zone Labs, Symantec's Norton Personal Firewall, Kerio, Tiny softwares Personal Firewall, Mac OS X, Windows 7, and above.

(Refer Slide Time: 12:39)



Living in a Wireless World

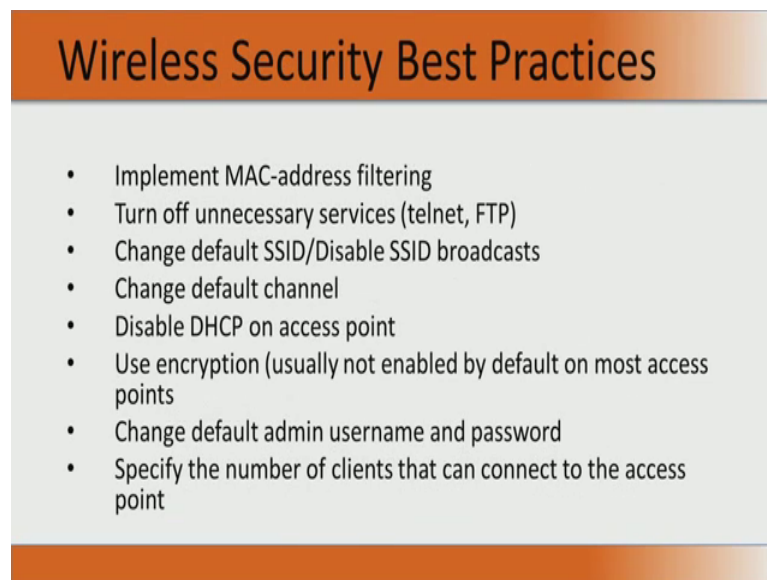
- Virtually all notebooks are wireless-enabled
- Serious security vulnerabilities have been created by wireless data technology:
 - Unauthorized users can access the wireless signal from outside a building and connect to the network
 - Attackers can capture and view transmitted data (including encrypted data)
 - Employees in the office can install personal wireless equipment and defeat perimeter security measures

We are also living in a wireless world. Virtually all the note books, your Ipad, Iphone, everything are wireless enabled. That means it assumes a WLAN access point to be available in the office. Now, having a WLAN will lead to very serious security vulnerabilities. Three of them I have listed here. One thing is unauthorized user can enter into a system because your wireless LAN is not bonded by the cable and it is unbounded by the air. So, some attacker can basically get into the access to the wireless signal from outside a building and actually connect to the network. So, you need to protect. An

attacker can also since is not going through your wired medium, the attackers can also capture and view transmitted data.

Very quickly today the employees in the office can install personal wireless equipments. So, your mobile phones can become a hot spot. So, any laptop can connect through the wireless to the mobile phone and the mobile phone will help them reach the internet through them. So, that a particular office says that though it says that wireless it has a password etcetra, it is not easy. Actually employees can use this wireless LAN though you have put all perimeter security. Since the wireless just not have very fixed perimeter, so people can use these wireless capabilities to connect and defeatperimeter security measures.

(Refer Slide Time: 14:46)

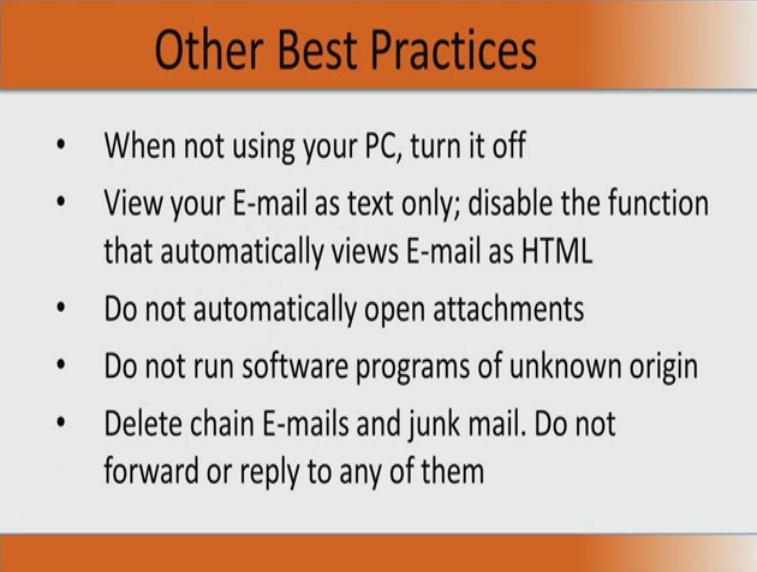


Wireless Security Best Practices

- Implement MAC-address filtering
- Turn off unnecessary services (telnet, FTP)
- Change default SSID/Disable SSID broadcasts
- Change default channel
- Disable DHCP on access point
- Use encryption (usually not enabled by default on most access points)
- Change default admin username and password
- Specify the number of clients that can connect to the access point

So, some of the best wireless security practices when you have a wireless LAN is to go and implement MAC address filtering, turn off unnecessary services, change default SSID, change default channel, disable DHCP on access point. You can also use encryption, change default admin user name and password, and specify the number of clients that can connect to the access point. So, all these things are some very important best practices for wireless security.

(Refer Slide Time: 15:28)

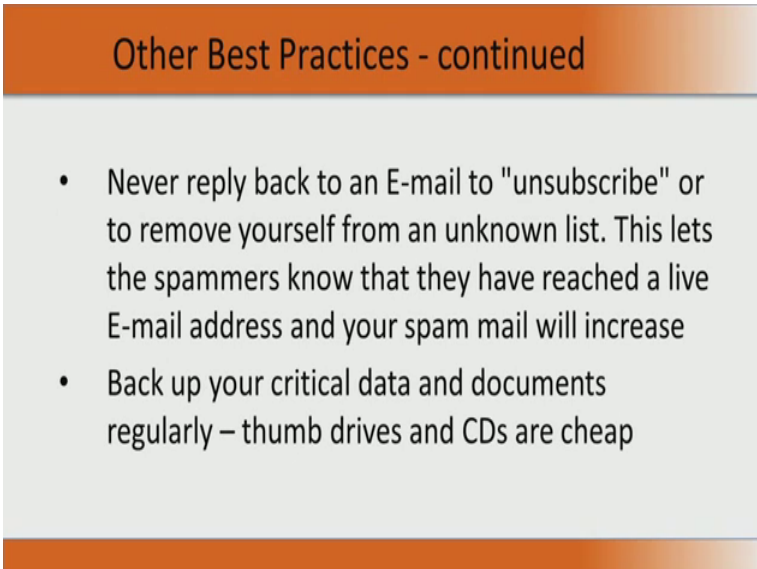


Other Best Practices

- When not using your PC, turn it off
- View your E-mail as text only; disable the function that automatically views E-mail as HTML
- Do not automatically open attachments
- Do not run software programs of unknown origin
- Delete chain E-mails and junk mail. Do not forward or reply to any of them

Some of the other best practices when not using a PC is turn it off because more you expose the PC to the internet, more would be the exposure of your to an untrusted environment. You need to view email as text only because that will disable the function that automatically views email as HTML, do not automatically open attachments, do not run software programs of unknown origin, delete chain emails and junk mail and do not forward or reply to any of them.

(Refer Slide Time: 16:13)



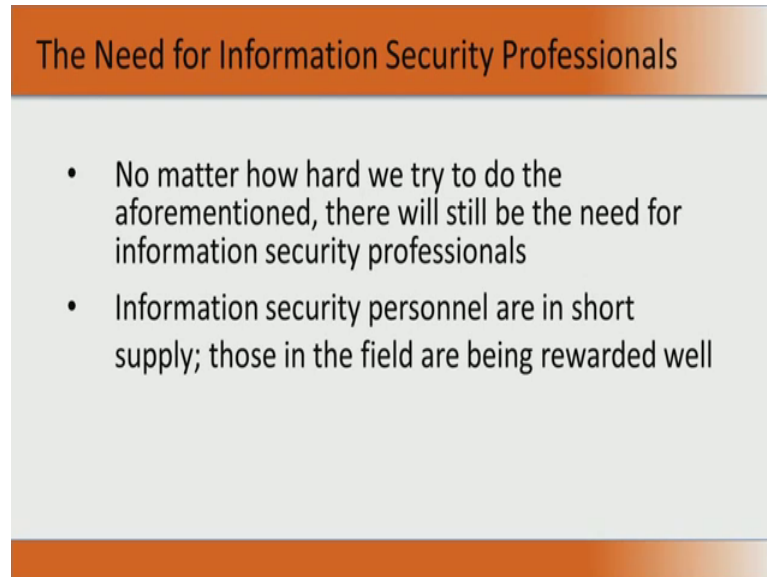
Other Best Practices - continued

- Never reply back to an E-mail to "unsubscribe" or to remove yourself from an unknown list. This lets the spammers know that they have reached a live E-mail address and your spam mail will increase
- Back up your critical data and documents regularly – thumb drives and CDs are cheap

So, these are all some best practices by which you can and very importantly never reply to an email to unsubscribe or to remove yourself from an unknown list. This lets the spammers know that they have reached a live email address and your spam mail will

increase, and back up your critical data and documents regularly. Thumb drives and CDs are actually cheap, so you can do that.

(Refer Slide Time: 16:39)



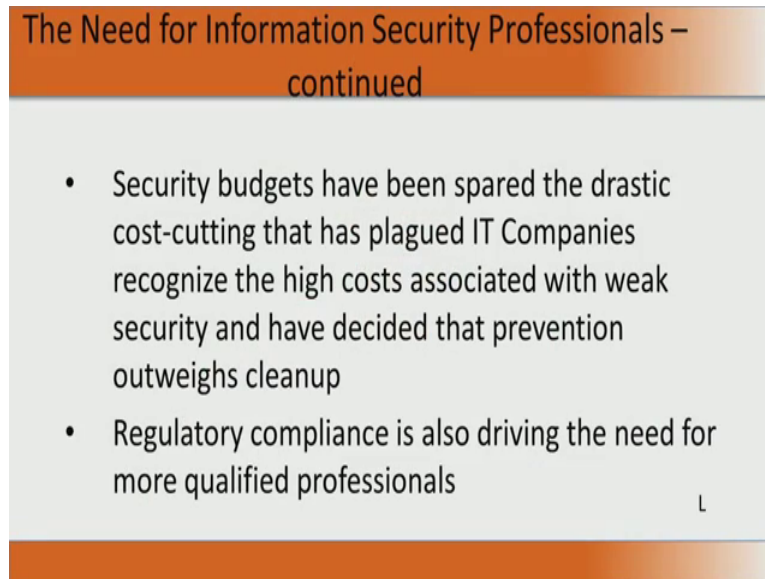
The Need for Information Security Professionals

- No matter how hard we try to do the aforementioned, there will still be the need for information security professionals
- Information security personnel are in short supply; those in the field are being rewarded well

We now look at why we are conducting this course. We have been telling you that there is a large need for information security professionals. Now, this slide basically talks of why we need information security professionals. We have been talking of implementing patches, implementing anti-spy ware, anti-malware etcetra. No matter how hard we try, this is not possible for user to do this rigorously. So, there is a need for information security professionals who understand the depth of the problem, the importance of this problem and they basically come and start installing this. They maintain the security within the organization, they maintain all the PCs and ensure that they are all secured, all the anti viruses are updated, all the spy ware, anti spy ware are all updated.

Now people who can appreciate information security, people who can do this meticulously, it is a skill and that skill set is what is lacking, long way in the market. There is a large shortage of secured information security personnel. So, if you become one, you actually become much more relevant to current days' most important problems, namely information security. Since, you become very much relevant to the most important problem today, you actually get rewarded very well for this. So, there is a need for skilled information security professionals and this course actually aims to motivate you to become one.

(Refer Slide Time: 18:51)



The Need for Information Security Professionals –
continued

- Security budgets have been spared the drastic cost-cutting that has plagued IT Companies recognize the high costs associated with weak security and have decided that prevention outweighs cleanup
- Regulatory compliance is also driving the need for more qualified professionals

L

Off late even the regulatory bodies have been talking about having qualified professionals who can ensure a secured operation within the organization, and even when you look at many IT driven companies, the security budgets have grown. They recognize that there is high cost involved, is associated with implementing security and security is a necessary prevention. So, many many organizations have started increasing the security budgets and they are looking for good information security professionals.

So, to sum up what we have done in this part of module 1 is that we have looked that a PC and we went and found out what a PC can do, how a PC can become a source of a malware, a source of nuisance to its neighbors, how a PC can become an nasty one in the internet which is an ocean of personal computers. So, we also have different type of current day attacks and solutions to this current day attacks, and many of the solutions needs to be meticulously done. There is not big challenge, there is no big intellectual activity involved, but the challenge is to be meticulous and the challenge is also that the intellectual challenge here is to go and come out with softwares, actually antivirus spy ware etc,i anti-spy ware etcetera which can envisage what could be the attack of tomorrow and make the prevention mechanisms today.

So, this actually requires more thinking. So, it is more artistic, it needs more imagination. I should imagine about what will happen tomorrow, what would be the possible security threats and the imagination needs to be wide, probably very unreasonable imaginations day dreaming may help. So, I just remember this say mid 1990s when the mobile phones came into existence, nobody ever thought that this mobile phones would be used for any

other purpose other than talking, but today you rarely talk on your mobile phone. You actually message, whatsapp and so many things. So, in some sense the functionality of a mobile phone has now become, the mobile phone turned out to be an organizer carrying some of the information, then it become almost a tablet today and almost a computer. People can actually now install shell and start even doing c programming on the mobile. There are processors that are capable of doing this.

So, the functionality, this is the wild imagination by person in 1995 if you had imagined that a mobile phone can be used for all these things. It would have essentially been a very wild imagination in 1995 or 96 when these mobile technologies started coming into place. Similarly, today we need people, the information security professionals who have understood the entire system today; and now go and see what would happen to these systems from a security point of view 10 to 20 years later and that will be very interesting exercise. You start making preventive measures for those types of vulnerabilities that could come years after would be a very big value addition. So, the role and need for information security professionals is going to grow on higher side in the next even 1 or 2 decades. So, take this course very seriously and try to become an information security professional to have a great career and a good service to mankind. We will now see in the next session about cloud computing.

Thank you.