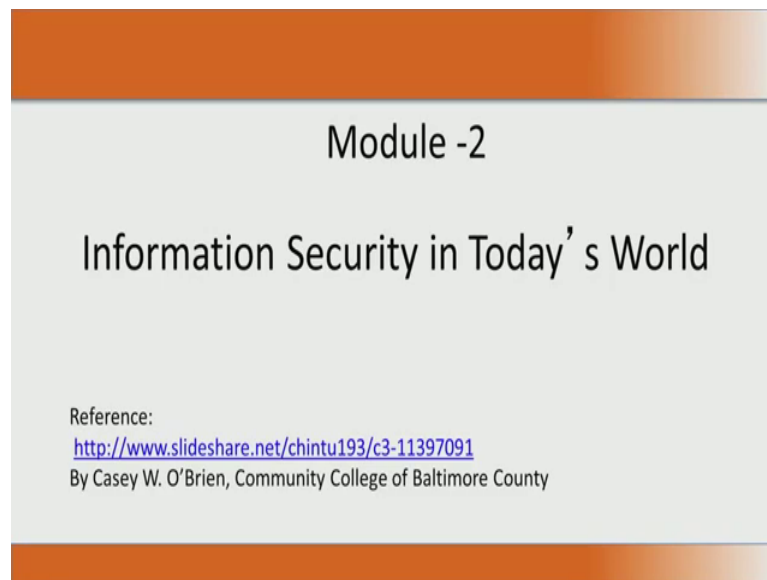


Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 18

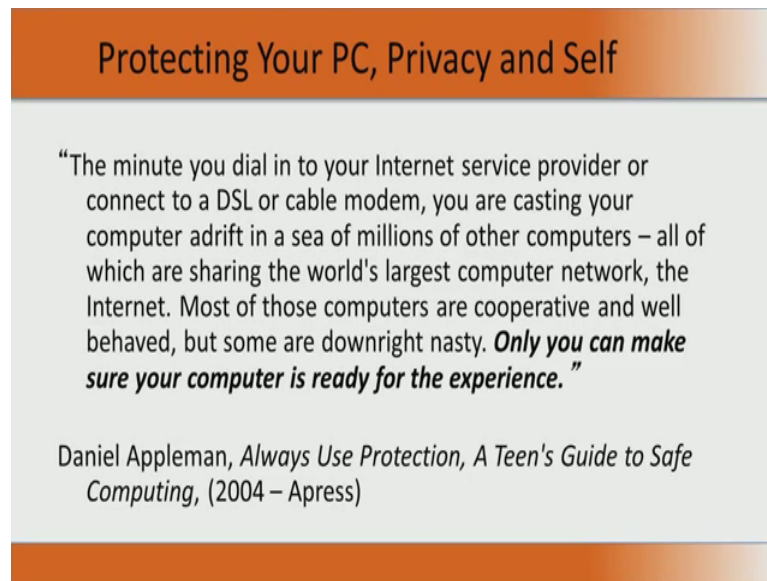
Brothers and sisters we will now see Module 2 of the course [FL]. In the module 2, we will consider and discuss more about information security in today's world.

(Refer Slide Time: 00:57)



We acknowledge Casey Brien from the Community College of Baltimore County. Some of his slides from the slide share we have used in this presentation. So, the very famous statement the minute you dial into your internet, your computer is actually exposed. You are actually pushing your computer into an ocean of many computers and that is where namely the internet and that is where vulnerability starts. So, this has to be kept in mind the moment you log on and connect your computer to the internet.

(Refer Slide Time: 01:43)



Protecting Your PC, Privacy and Self

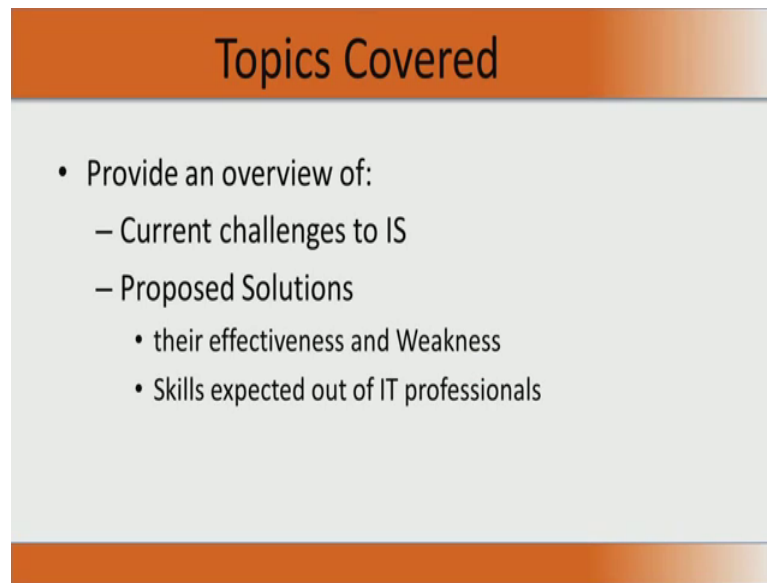
“The minute you dial in to your Internet service provider or connect to a DSL or cable modem, you are casting your computer adrift in a sea of millions of other computers – all of which are sharing the world's largest computer network, the Internet. Most of those computers are cooperative and well behaved, but some are downright nasty. **Only you can make sure your computer is ready for the experience.**”

Daniel Appleman, *Always Use Protection, A Teen's Guide to Safe Computing*, (2004 – Apress)

The moment you say dial up or the moment you connect to a broadband, immediately you should understand that now your system is not a standalone system that is one in a million and you need to look at protecting your personal computer. You should ensure your privacy and also your identity. This was a very famous statement. I will just read this statement. The minute you dial into your internet service provider or connect to a DSL or cable modem, you are casting your computer a drift in a sea of millions of other computers-all of which are sharing the world's largest computer network internet. Most of those computers are cooperative and well behaved, but some are downright nasty. Only you can make sure your computer is ready for the experience. So, this was by Daniel Appleman in his article, *Always Use Protection, A Teens Guide to Safe Computing*.

So, in this module we will basically talk about how to protect your personal computer, what are all the simple things that you need to do technically to protect your personal computer, so that you are not bothered by the nasty computers that are there along with you in the internet, and at the same time you do not allow your computer to become nasty through unauthorized software being installed and trying to cause some issues. So, that would be the first part of module 1 protecting your personal computer.

(Refer Slide Time: 03:49)

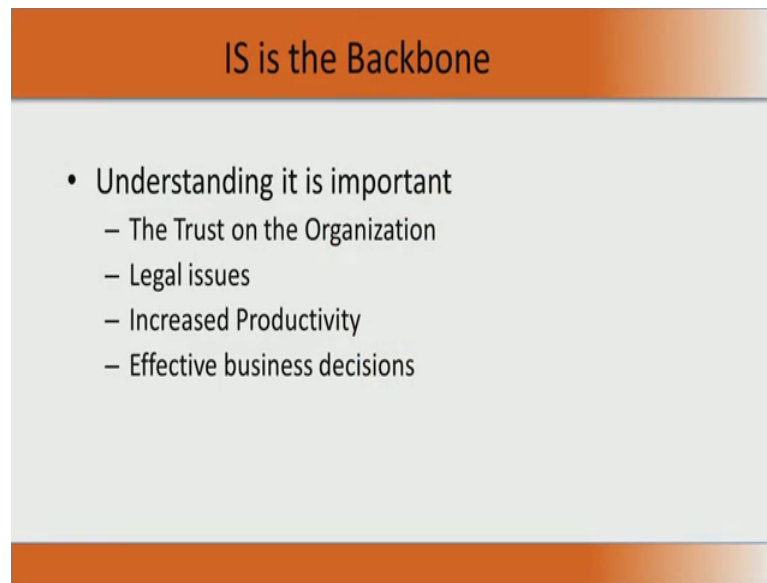


The slide features a title bar at the top with a gradient from dark orange to light orange, containing the text "Topics Covered" in a bold, black, sans-serif font. Below the title bar is a light gray rectangular area containing a bulleted list. The list starts with a main bullet point "• Provide an overview of:", followed by two sub-bullet points: "– Current challenges to IS" and "– Proposed Solutions". Under "Proposed Solutions", there are two more sub-bullet points: "• their effectiveness and Weakness" and "• Skills expected out of IT professionals". The slide concludes with a solid orange horizontal bar at the bottom.

- Provide an overview of:
 - Current challenges to IS
 - Proposed Solutions
 - their effectiveness and Weakness
 - Skills expected out of IT professionals

The way we go about this particular part of module 2 is you look at the current challenges in information security. The current challenges specifically from the point of view of a personal computing machine and then, you will look at some of the proposed solutions. You will look at how effective are these proposed solutions in addressing the problem of security and also, some of the weakness and then, we will also look at what are the skills that we expect out of IT professionals of different levels. IT professional who just use the system for doing certain activities, IT professional who develop software; IT professional who maintain data, custodians of data. So, the different profiles of IT professionals and the skill sets from a security point of you, we will also look at it in some detail during this lecture.

(Refer Slide Time: 04:51)



The slide features a title bar at the top with a gradient from dark orange to light orange, containing the text "IS is the Backbone". Below the title bar is a light gray rectangular area containing a bulleted list. The list starts with a main bullet point "• Understanding it is important", followed by four sub-bullet points: "– The Trust on the Organization", "– Legal issues", "– Increased Productivity", and "– Effective business decisions". At the bottom of the slide is another gradient bar, matching the top one.

- Understanding it is important
 - The Trust on the Organization
 - Legal issues
 - Increased Productivity
 - Effective business decisions

Note that information system is the backbone of any organization and you need to understand its importance because a flaw in that would essentially removes the trust on the organization, basically the customers trust on the organization. It can cost major legal issues. If you have a good understanding, your organization can show a better productivity and it also helps you in taking very effective business decisions. Your business decision is based on the information that you have; the capability for you to interpret raw data in a meaningful manner, so that it could influence your business decisions. If you have security, you are very sure that your data is, there is an integrity in your data and only authorized people have access to it, so if you have a data with lot of integrity, then it can certainly help you in making correct and effective business decisions.

(Refer Slide Time: 06:00)



So, now looking at an organization where there are lot of people and we need to secure people. How do we secure these people? We go and make their end machines, the client machines or their PCs very secure and that is why we started talking about, it is not just the PC that you use at home, it is also the PC that you use at office. How do you go and secure this PC? What is the main challenge? What are the main challenges, technological challenges that will make your life complicated, that will make securing a PC very difficult?

Now, let us look at that in a little more depth. Number 1 is today attacking a system has become fast. Fast from two angles. One thing is internet has become very fast. So, if a worm has to spread, it can spread at giga bit speed or tera bit speed. It has large pipe line where the worm can now spread though the internet has expanded, has grown in capacity in terms of bandwidth and through put over these years for the benefit, so that we access information fast, but the flip side of it is that in an unsecure network, virus can also spread very fast. Similarly, the other way of attacking is to go and decrypt your key or go and look at quickly guess your password. Your password has to become stronger and stronger because now the compute speeds are quite high. The cost per million instructions per second is sub dollar today. So, you have machines with lot of memory and lot of processing power with more than 1 core or CPU core in a small chip today. Even your mobile phones come with either two CPUs or four CPUs. You call it as two core or four cores quad core or dual core.

So, we think with such type of increased speed, one can quickly go and do even a

slightly naive things like brute force method and break your password. They can go and break your cryptography; they can go and break your encryption. So, that is also another vulnerability; that is also another challenge to it. So, the speed of the internet and the speed of the system today cost post major challenge for you to contain, prevent, avoid viruses. The next thing is there is lot of sophistication in attacks. People have started understanding. Suppose you look at an operating system, they runs on millions of lines of code and it is practically impossible for us to look at the entire one million line of code and look for vulnerabilities there. So, people now start understanding many of these and they could come out with more sophisticated attack. So, these naive attacks have gone. If you want to understand an attack, it takes quite a bit of time. Probably it can become for you to one month lecture to go from basics to understand an attack.

So, the attack, sophistication of attack has indeed become much more complex, and there is also a very quick detection of weaknesses. Suppose software release today within days, not even weeks; within days. Within a week all the vulnerabilities of that essentially are understood and this is mainly because we have large compute power to go and look into the system. Now, the other issue is that the attacks are not originating from a single place. If it is originating from a single place, then it is probably easy to see to go it contain it. Now, we have something like a distributor attacks. Attacks can originate from different place and attack different destinations. It is not a single source and single destination; it has multi source and multi destination attack. Suppose I understand that there is vulnerability, there is a virus going around in the internet and the softwares I use may have made patches to stop the virus from affecting the system. Now, there are lot of difficulties in actually going and patching. We will list some of the difficulties as we go through this lecture and that is another technology challenge.

So, increase speed of internet and computers, more sophistication in attacks, faster detection of weaknesses by the adversary distributed attacks and difficulties of patching, pose severe technological challenges today to address even the last end mail security, namely security of the client machine or the personal computers that users use to connect and do the computing.

(Refer Slide Time: 11:49)



Now, given all these challenges, what are all the different ways by which the PC can be attacked? It can be an identity theft where your password, your personal information is compromised. It can be a malware. Your software is malicious software or it can be patch management failures. Patches from a security point of view or put to see that certain vulnerabilities are removed, or the certain vulnerabilities are addressed. So, there are some ways, there are many valid reasons, many practical reasons for how a patch management could fail. Another interesting thing is the distributed denial of service or D-dos. So, these are all very commonly reported in the recent past and today as some of the latest attack trends. Now, we will look at these trends namely identity theft, malware, patch management failure and D-dos in some detail as you proceed.

(Refer Slide Time: 13:05)



Latest Trends - Identity Theft

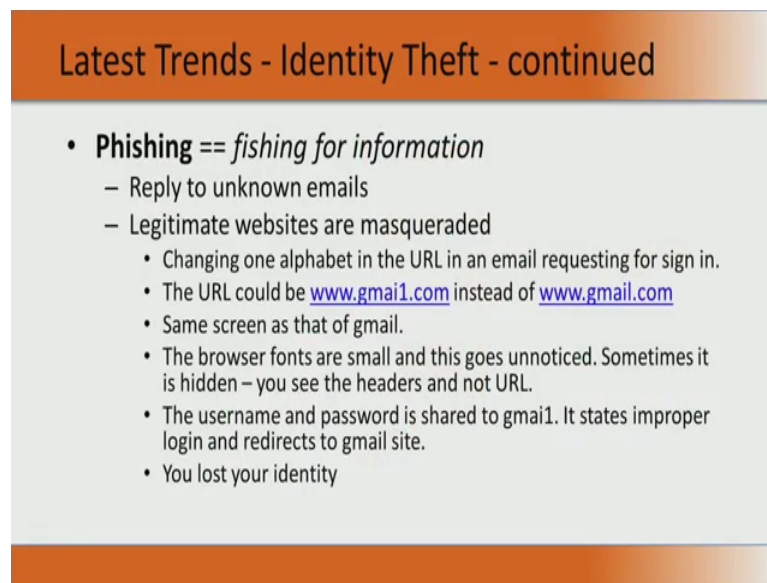
- Crime of the 21st century
- Damage is more than just losing money
 - Credit rating,
 - “Bad” emails
 - Loss of Access to Accounts
 - Manipulation of data before retrieval
- Loss of Confidentiality, Integrity and Availability

Identity theft, going and finding somebody's password and user name and password is the crime of the 21st century and what you lose when you lose your password or when you lose your user name password. One of the things the simple or the very quick damage one can do and the reason why this is being done today? Why it has become a crime is that people once they steal the identity, they go and do something with your money. They go and purchase something from your credit card; they change your email id. Then, what happens is ultimately you have not purchased anything with your credit card. So, you do not go and pay anything, but then over a period of time you get a notice and your credit rating is spoiled. So, you need to spend lot more time to go and tell. So, tomorrow you go for a loan, your credit rating may be not good and banks may deny loans.

The other damage so you have to fix your credit rating. So, these are something, which are quite common nowadays. There are bad emails. So, they log in to your account and send a very very quote and quote bad email which can land you up in unimaginable problems and you may lose access to your accounts meaning you lose access to your data. You will lose access to what all you have done. For many emails is an account of what they have done. Email is the information that they have if they lose the emails; they lose a lot of information. So, loss of access to account and it can also be a banking account and you lose access on a week end and so, you need to wait for two days to get back your access to the account. So, there is certainly is security vulnerability because it comes under the availability of the CIA which is the three goals of security.

One another thing is that, I can go and manipulate the data if they get access before retrieval. So, if you look at these four points of what identity theft could damage, you'll actually lose all the three. You lose confidentiality and since you lose confidentiality, your data can be changed. So, the integrity is lost and then one can go and change your password and make things not available to you. So, there can be an availability issue. So, confidentiality, integrity and availability are basically the three goals of security. All these three courses can be compromised the moment I have an identity theft.

(Refer Slide Time: 16:09)



Latest Trends - Identity Theft - continued

- **Phishing == fishing for information**
 - Reply to unknown emails
 - Legitimate websites are masqueraded
 - Changing one alphabet in the URL in an email requesting for sign in.
 - The URL could be www.gmai1.com instead of www.gmail.com
 - Same screen as that of gmail.
 - The browser fonts are small and this goes unnoticed. Sometimes it is hidden – you see the headers and not URL.
 - The username and password is shared to gmail. It states improper login and redirects to gmail site.
 - You lost your identity

One another very interesting way of stealing identity of getting your log in and password say of your Gmail account is by what we call as phishing. So, phishing is nothing, but fishing for information. So, how does this come? One of the thing is we get an unknown email which is sort of very disturbing. We will see do not the line there was a virus which said from here is a mail from some FBI and you have accessed the illegal sites. So, immediately tell your log in and password, so that we see that you do not land up in problem. You get really perturbed and you send all your details. So, one of these emails we will see if one such very interesting case study down the line.

The other interesting thing in nowadays when you see browsers specifically in your mobile, the exact URL does not come on the URL link whether some header comes there. Now, people have been playing with this URL to actually steal information, actually steal identity. This is one example as you see on the screen. So, we send the email and say now log in to your Gmail by clicking here and when you click here that place instead of going to www.gmail.com, it can go to www.gmai1.com, the numeral 1.com

and since fonts are small and probably you do not really look into closely, you may think that the first one www.gmail.com looks like gmail.com. So, you go and click there and what happens there, the exact screen of Gmail is actually put in that www.gmail.com. So, you go and log in and give your password. It looks exactly like Gmail. So, moment you give your log in and password, then immediately you press the submit button.

Then, the software in the web software is configured in such a way that it says wrong log in password incorrect and take you to the original Gmail page, redirects to the original Gmail page. Before it redirects to the original Gmail page, it actually stores the user name and password before redirecting to the original Gmail page. So, what happens there when you go the next time, we go to the original Gmail page, you go and put your user name and password, it automatically logs in. So, what you think is because password also is not shown on screen may be you think you have entered the password wrongly and you do it next, but what has happened here is that you did not go to gmail.com.

To start you went gmail.com. There you gave user name and password that fellow stole it and then redirected you to gmail.com, original gmail.com with a message that you entered wrong password and you go there and log in and go. So, you do not notice that you have done something here and when it goes unnoticed, the hacker can basically get your identity, your user name and password. So, by this what happens is, you actually have lost your identity.

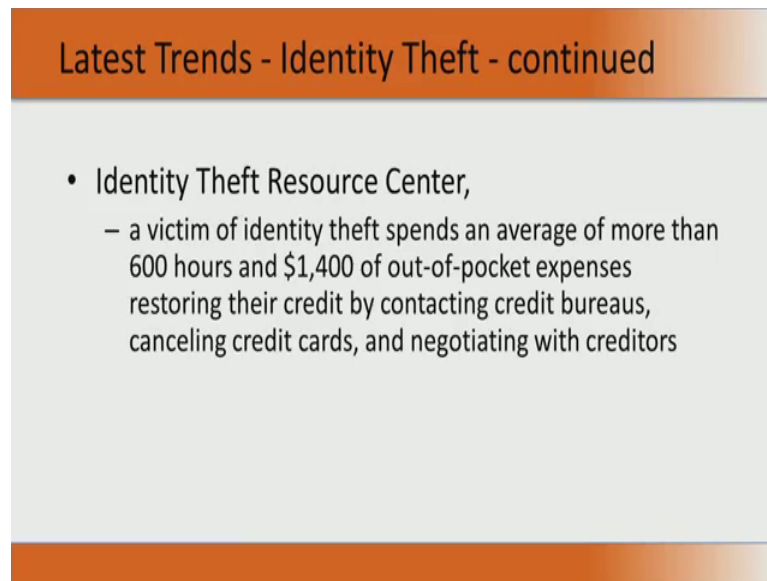
(Refer Slide Time: 20:47)

Modern "Deewar" dialogue

- The original
 - Amitabh: "Mere Paas bungalow hai, gaadi hai, Bank Balance Hai, kya hein tumhare paas?"
 - Shashi Kapoor: "Mere paas Maa hai"
- Today's Deewar
 - Amitabh: "Mere Paas Antivirus hai, firewall hai, broadband hai, credit card hai, kya hein tumhare paas?"
 - Shashi: "Mere pass tumhara PASSWORD hai Baayi"

So, this is a very interesting simple case study that is reported well in the literature. Whenever we think of identity threat, I remember the movie Deewar-Amitabh Bachchan and Shashi Kapoor. So, there is a famous dialogue there. Amitabh says [FL]] and Shashi Kapoor replies (20:43- FL). We look at today's Deewar [FL]. I hope you will not lose your password.

(Refer Slide Time: 21:14)



Latest Trends - Identity Theft - continued

- Identity Theft Resource Center,
 - a victim of identity theft spends an average of more than 600 hours and \$1,400 of out-of-pocket expenses restoring their credit by contacting credit bureaus, canceling credit cards, and negotiating with creditors

What happens if you lose your password? This is a survey done by the identity theft resource center. Note that there is the resource center for identity theft. It was found out 2 years before report that a victim actually spends an average of more than 600 hours and around 1400 dollars out of pocket expenses to restore their credit by contacting credit bureaus, canceling credit card and negotiating with creditors proving that there was an identity theft and they were not responsible, and at least not get a bad negative report for their credit rating. So, this is one very important thing that the people have to keep it mind. So, password has to be a password and it has to be maintained nicely. In a next session, we will see about other technological advances and other viruses, namely the malware.

Thank you.