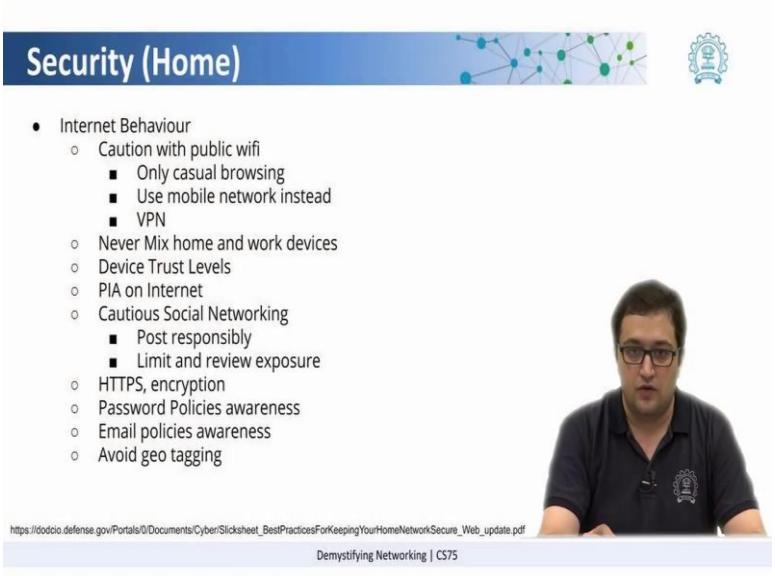
Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 84
Responsible Behavior on the Internet

Now, the next topic that we will look at is called internet behaviour. So, what are the kind of things that we could do which will ensure us to be safe on the internet.

(Refer Slide Time: 00:11)



The first thing is when we use public Wi-Fi networks, we should use only use it for casual browsing; that means, do not do financial transactions on public Wi-Fi because you do not have control over what are the kinds of things that are working on that particular network. There might be people who are trying to sniff the network for say different purposes and there could be malicious users who could use this information against you.

Then the other thing you could do is use mobile networks instead because your mobile network is directly connected to your internet service provider which is a much more secure network than a public Wi-Fi network or what you could use is something called a VPN or Virtual Private Network. A simple VPN software what it does is it creates a tunnel between your system and the VPN server and this tunnel is encrypted. So, any information going through it is in an encrypted form. Hence, others on the Wi-Fi

network will not be able to look into the kind of information that you are communicating on the network.

So, the next point that we look at it is never mix home and work devices. So, why not do that? Because your work devices have access to certain networks and say certain confidential applications. And, if you have to happen to be browsing some websites which had malicious code on your work device, that could compromise the security of the entire network of the company.

So, the best practice is, you can access it over your personal device because the level of damage that might happen could be limited to just that device versus the entire company's network being compromised. That is why companies have a policy where you can you are not allowed in certain cases to take the devices home and even if you are you are not allowed to do private browsing or say social networking on your work laptops or say other devices.

Then you should also have device trust levels as we talked about. So, if a device is being used say by the kids and who are not that that much aware of security might browse some interesting games websites, but which might have some malicious code which could have been installed on that system. So, it would not be advisable to do something say like a financial transaction on that particular system as it could lead into leakage of your private information.

So, other thing that you should be aware of is called the PIA or Personally Identifiable Information on the internet. This means that a set of information that can identify you as a person for example, your date of birth your address and a lot more things.

Now, these information are also used as authentication measures by some of the important organizations say your office or your bank. For example, when you call your bank they usually asks you what is your address or what is your email ID that is also a level of authentication that they are trying to do.

But if you have all these information available in one place or the internet, this information can be used against you or can be used by a malicious person to pose as you. In regards to PIA what we have to be cautious about is when you are using social network. You should post very responsibly and be aware of the kind of things you are

posting, and you should also review the kind of things you are posting so, that the PIA is limited

For example, if there is certain information which you feel can be used against you it should be limited say between your trusted group say just your friends. The other thing that you should be cautious about is use https while browsing, you should have you should be aware of the password policies like you should change your passwords say in a month or two or if you feel that a password has been compromised or you have shared the password with a lot of people, then it is a good time to change your password. You should also be aware of the email policies like we were talking about the classification of information.

For example, if you are sending this email as a secret to the other employee on the same company, you might want to mention it as a secret or whatever the classic classification terms that are used in your company. Then another point that you should be aware of is avoid geo tagging. So, these days many phones they come with a feature of recording your GPS coordinates, when you take a picture. So, you should be aware that when you are sharing the pictures maybe the information about your location is also getting shared.