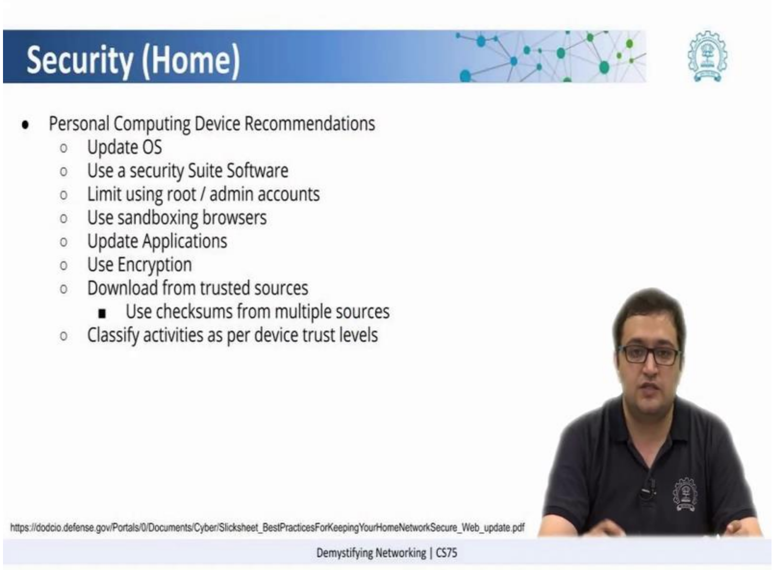
Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 83
Personal Computing Device Recommendations

Now, this brings us to the last topic that we want to discuss in security which is basically certain practices that we can follow at home to ensure a secure communication and secure network. So, what are the things that we can do?

(Refer Slide Time: 00:17)



Security (Home)

- Personal Computing Device Recommendations
  - Update OS
  - Use a security Suite Software
  - Limit using root / admin accounts
  - Use sandboxing browsers
  - Update Applications
  - Use Encryption
  - Download from trusted sources
    - Use checksums from multiple sources
  - Classify activities as per device trust levels

https://dodcio.defense.gov/Portals/0/Documents/Cyber/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure_Web_update.pdf

Demystifying Networking | CS75

So, let us look it in parts. So, the first part is the personal computing device recommendations, which basically means, what are the recommendations for the devices that you have, that you communicate with over the network.

So, the few things that you should take care of is, update your operating systems, use security softwares, limit the use of route and administrative accounts because if those are compromised it becomes easier to access your system, then use sandboxing browsers. So, what we mean by sandboxing browsers is, these browsers, they work in an independent environment and in case there is a malicious code that has been executed, it will just affect the browser and not the system.

So, there are lot of sandboxing browser that are available and a lot of browsers have the sandboxing capabilities. You should also update the applications that you are using, use encryption wherever possible for example, use https ensure all your websites that you are using are one HTTPS, then you should always download software from trusted sources.

For example, if you are say you are trying to download VLC media player, you could go directly to the website and download it from there. And, if even if you are downloading it from say a different source there is something called a checksum which is available with every software. You could copy the checksum from the website, download the software and use any simple software to calculate the checksum of that particular application or the file that you have downloaded. If these two match then; that means, you have the correct software and it has not been tampered with.

And the last point in this section is classify activities as per device trust level. So, what we mean by device trust levels? So, you have a lot of devices say one device is used by your children in the house, some are used by you. So, children are not that aware and they might go into websites which might compromise their systems. So, try not to use those systems for say financial transactions. So, every device can have a different trust level based on who is using it, how much that particular user is aware. So, you should know which applications or which particular functions you should not perform or perform on those devices.