

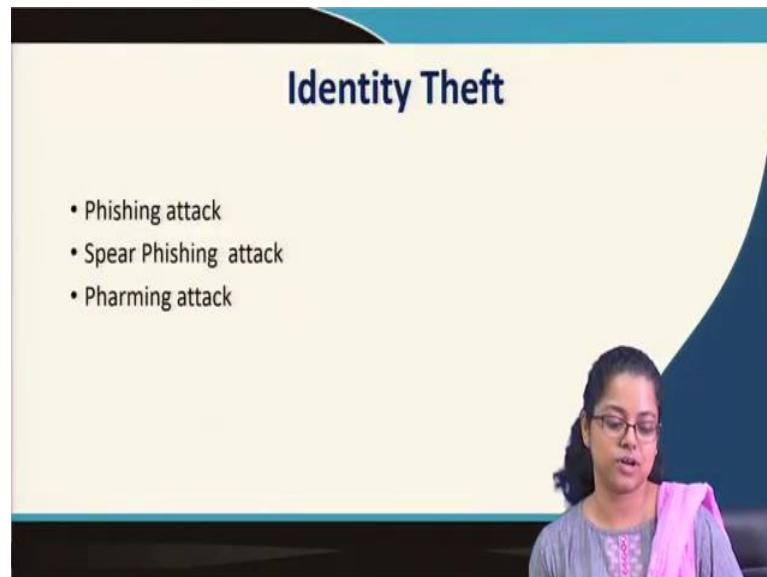
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module – 11
Ethical, Social and Security issues in MIS
Lecture - 54
Security Issues in MIS – II

Hello, welcome back! So, in the previous session, in this module, we had spoken about security breaches and we had discussed about the different categories of security breaches. We had begun talking about man in the middle attack, and we had discussed denial of service attack and some other kinds of security breaches.

So, in this session, we will discuss about some other security breaches which are very-very relevant in today's world. And then, we will move on and we will talk about counter measures or solutions to those security breaches.

(Refer Slide Time: 00:57)




So, let us see the other security breaches that are there in the world around us. Identity theft, very-very critical kind of information security breach that troubles the entire world around us. An identity theft has become more and more you know critical with the arrival of online or a digital modes of transaction E-commerce and the digital world

right. So, what are the different kinds of identity theft breaches? The first one that we will talk about is phishing attack and then, spear phishing and finally, pharming attack.

So, let us see what a phishing attack is. I am sure you would have heard of phishing attack or you might be familiar with what a phishing attack is. Because today you know many websites especially banks, they would warn you or alert you about a phishing attack; because phishing attacks have become very very predominant or prevalent and they are very dangerous.

(Refer Slide Time: 01:59)



Phishing Attack

- Attacker sends e-mail messages to a large number of recipients
- Message states that an account has been compromised and the matter should be corrected
- Message includes a link which takes the user to a fake site that resembles the authentic site.
- User enters a login name and password and gets an error message.
- Perpetrator captures the user details.
- Once inside a victim's account, the perpetrator can access personal information

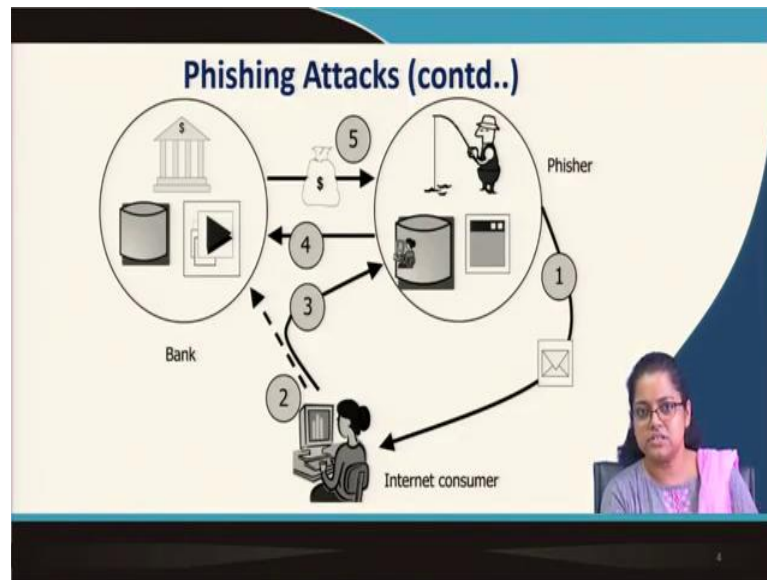
The slide features an illustration on the right side showing a fisherman in a boat casting a net into a body of water. In the water, a person is sitting at a desk with a computer, and a fish is being pulled towards the net. The word 'PHISHING' is written in the water near the person at the computer.

So, what is a phishing attack? It goes about like this. The attacker sends an e-mail a message. So, it is the attacker sends e-mail messages to large number of recipients. The message states that an account has been compromised and the matter should be corrected or rectified. Message includes a link which takes the user to a fake site that resembles the authentic website. User enters a login name and a password and gets an error message of course.

Now, once the user enters the login name or the, and the password, perpetrator automatically captures the user details. And once inside a victims account, the perpetrator can wreak havoc and can access personal information, can even you know I do not know what other details, what other details or you know you can the perpetrator can even transfer money, can do anything, can wreak havoc basically.

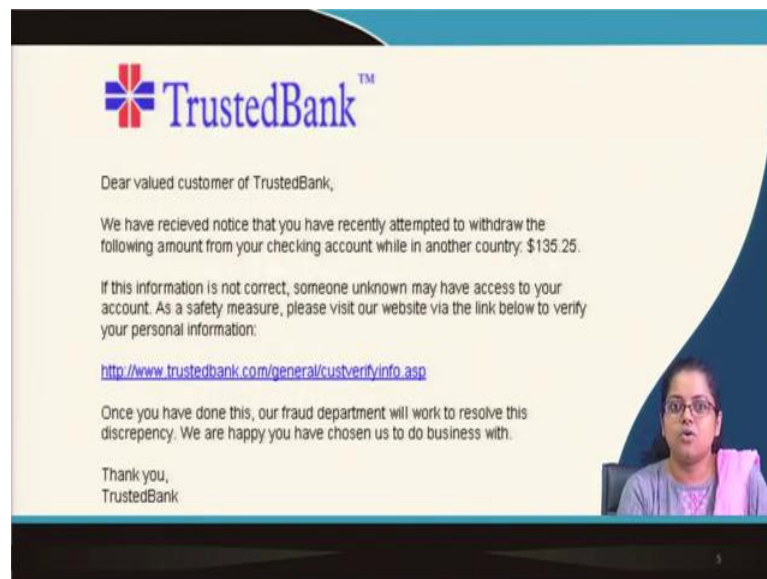
So, this is how a phishing attack works right. So, it all begins with an e-mail that is sent to a large number of recipients. And if the recipients are not alert and fall prey, they can go ahead, click the link and divulge their very-very confidential information and once the information is divulged, the victim is at the mercy of the perpetrator.

(Refer Slide Time: 03:27)



So, this graphically shows all the steps that we have just discussed in a phishing attack. I will not spend more time on this rather I will move on to other, you know, topic; so, alright.

(Refer Slide Time: 03:37)

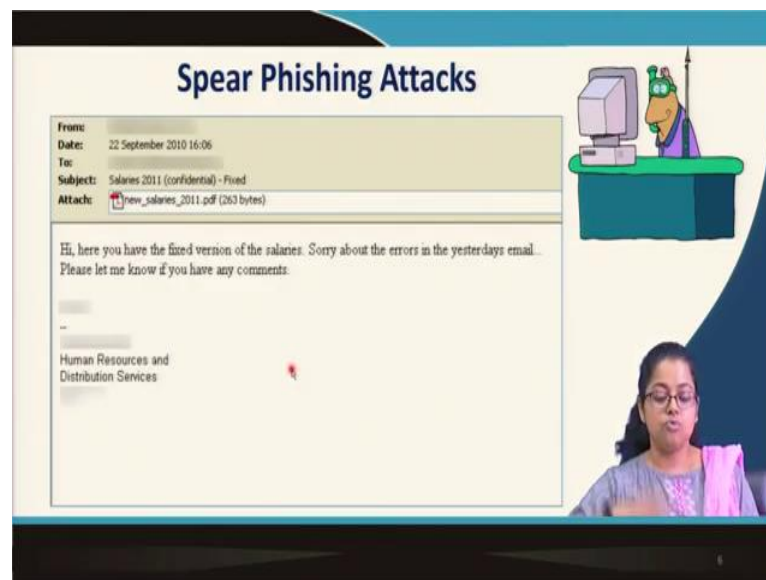


So, this is how a phishing attack is usually drafted. Please have a look here that we are talking about. It usually comes from an entity that you trust could be your trusted bank. Of course, this will have a name here. Now, and it would say that it would be crafted in such a manner that it would be crafted very cleverly so that a person who is not aware of what a phishing attack is there is a high probability that that person falls into the trap.

Here also you see that we have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country and look at the amount. So, of course, if you are not aware, you may feel that you have not been to a foreign country and the probability that you know of course, the probability that you have been to a foreign country is low and while in that country, you have transacted with this much amount of money is even lower.

So, if a person is not familiar with the fact, with what a phishing attack is, it is very easy to for the person to fall prey to this and the person may go to this link and divulge his or her personal information.

(Refer Slide Time: 04:46)



Now, moving on to a Spear Phishing attack, which is a variant of a phishing attack. As the name suggests here, we see a spear. So, a spear phishing attack is a targeted phishing attack because a spear is usually targeted at somebody. So, as instead of you know a phishing attack which is a very generalized e-mail, a spear phishing attack is a targeted

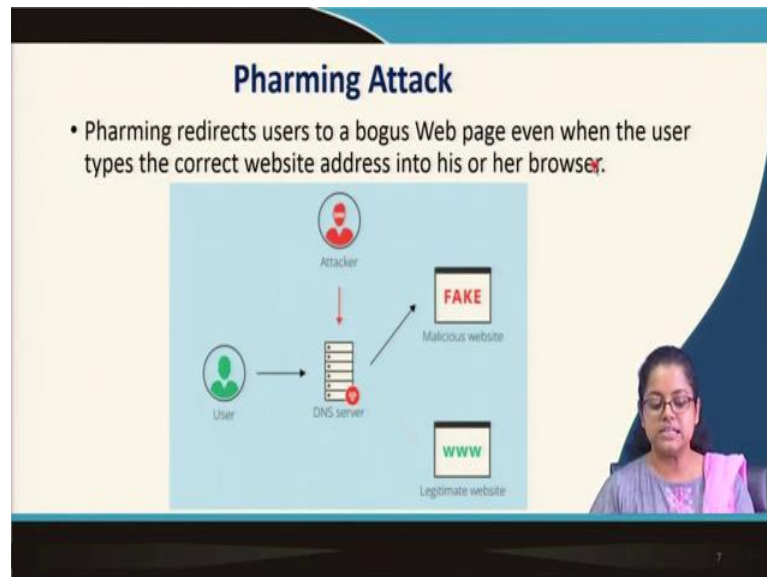
phishing attack sent to a particular individual and it appears to come from some within your organization or somebody whom you personally know.

So, here this is an example of a phishing attack usually phishing attacks pretend to come from within your own organization. So, in this case, the phishing attacks come from pretends to come from human resources and distribution services. So, it is mentioned here that high here you have the fixed version of the salaries, sorry about the errors in yesterday's email. Please let me know if you have any comments.

So, it since it appears to come from a trusted source, there is a very low probability that anybody would not trust this. If the person is not aware, they would obviously you know trust this and divulge his or her personal information and you know how touchy people are about their salaries.

So, if they see that there is something wrong in salary details, they would automatically go back and they would revert to with their actual salaries maybe. So, then their confidential information now lies with the phisher right. So, you see how spear phishing attack differs from a phishing attack and how this is more targeted.

(Refer Slide Time: 06:38)

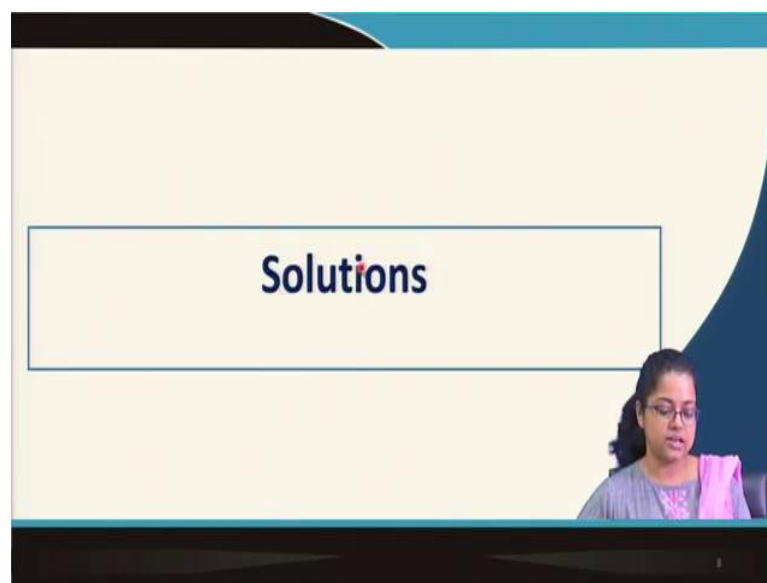


Now, coming to the next category of identity theft; Pharming attack. Pharming attack is again very very similar to a phishing attack, the only difference is pharming redirects

users to a bogus web page, even when the user types the correct website address into his or her browser.

So, here also the user is you know diverted to an incorrect web page. So, here you see what instead of going to the legitimate website, the user lands on the fake website. And in the fake website you can actually keep spyware or you can keep some you know you can ask the user to enter his or her details and again, you confidential user information lands in the hands of the perpetrator.

(Refer Slide Time: 07:24)



Now, we have discussed about phishing attacks, man in the middle attack, denial of service attacks, identity theft, malware and several other kinds of security breaches. So, now what are the counter measures? So, we will spend some time on solutions or counter measures to these security breaches.

(Refer Slide Time: 07:46)



Organizational security environment, this is very important because here we see a three layered, you know, defense. So, if there is data within an organization, there are three layers of defense or counter measures in order to protect your data from perpetrators or hackers or malicious entities outside.

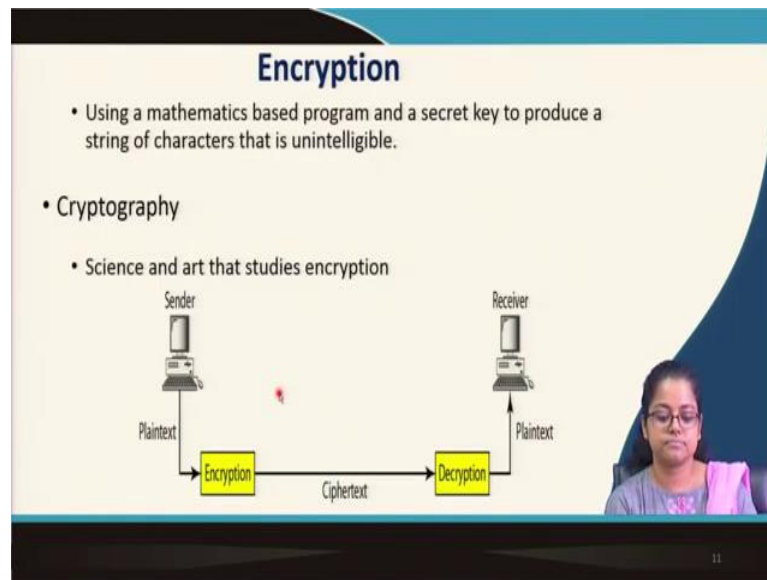
So, the first layer here pertains to technology solution. So, that is the first line of defense. The second line of defense is constructed by organisational policies and procedures and the final line of defense is when both of these you know fail, then you have to resort to laws and industry standards. So, this is the third and the final line of defense against security breaches.

(Refer Slide Time: 08:39)



Now, moving on, let us talk about each of these solutions in detail. So, the first solution here Technology solutions.

(Refer Slide Time: 08:47)



Encryption; so, encryption is the first solution technology solution that we want to discuss here. Encryption means encryption uses mathematics-based program and a secret key to produce a string of characters that is unintelligible. So, its un intelligible; therefore, it cannot be deciphered by a hacker or a malicious entity, unless the hacker also has ways and means to decipher it right.

So, cryptography, which is the art and science that studies encryption. So, cryptography means, it is a branch of study that is an, it is both science and an art that is used to study encryption. So, what happens in encryption here; let us; let us understand. So, there is a sender and there is a recipient.

The sender sends wants to send some message to the recipient, but the sender does not want any third party to intercept that which would happen in case of a identity theft or it can happen in case of a man in the middle attack. Where a man in the middle would actually try to intercept this information and alter it and maybe send an altered or manipulated version of the message to the, to both the parties or maybe to the recipient.

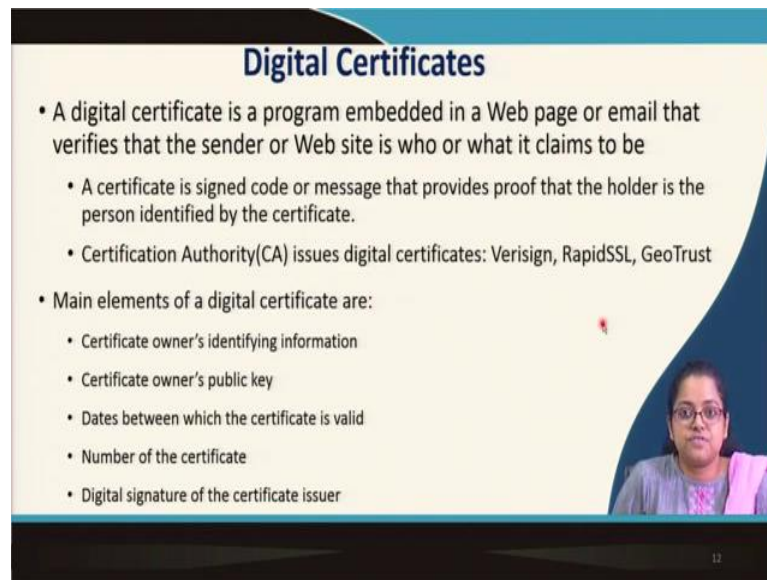
So, the plain text message which is the original message is encrypted and once so, there are a lot of encryption algorithms, we will not get into those because, those are a little technical in nature and may be beyond the scope of this course. But for the time being let us understand that there are some very simple also very complicated encryption algorithms; but there are some very simple algorithms also.

So, there are some algorithms which are used to encrypt the original plain text into a format which is known as the Cipher text. The cipher text is the encrypted message and this is unintelligible which we have mentioned here, it is unintelligible. So, it cannot be understood by anybody from outside any third party. Now, once it once the cipher text reaches the receiver or the recipient; again, it is decrypted and the recipient sees the original message.

So, here there is a concept of public key, private key and keys; but again, keys are a little technical in nature. So, will not get into a details of those, but so here because here we were speaking about a secret key, so there is a key, but, we will not get into the technicality.

So, it we will keep it simple by assuming that there is a plain text, which is encrypted and there is a cipher text which is which is the unintelligible message and once it reaches the recipient, it is again decrypted by using those keys. Encryption, decryption both happens by using those keys and once it is decrypted, the original message is visible to the recipient. This is how encryption works.

(Refer Slide Time: 11:53)



Digital Certificates

- A digital certificate is a program embedded in a Web page or email that verifies that the sender or Web site is who or what it claims to be
 - A certificate is signed code or message that provides proof that the holder is the person identified by the certificate.
 - Certification Authority(CA) issues digital certificates: Verisign, RapidSSL, GeoTrust
- Main elements of a digital certificate are:
 - Certificate owner's identifying information
 - Certificate owner's public key
 - Dates between which the certificate is valid
 - Number of the certificate
 - Digital signature of the certificate issuer

Now, moving on the next counter measure, technical counter measure that we want to discuss is Digital certificate. So, what is a digital certificate? A digital certificate is a program embedded in a web page or an e-mail that verifies that the sender or website is who or what it claims to be.

So, very important because it says that you know if there is a website and if it is claiming to be a website, a digital certificate actually verifies that. A certificate is signed code or message that provides proof that the holder is the person identified by the certificate.

And of course, the certificate is provided by certification authorities, who issue these digital certificates. And these certification authorities are very large players such as you know very popular players, who have a lot of credibility and that is the reason why the certifications that the certificates that are issued by them are considered to be credible. So, some popular examples are Verisign, RapidSSL, GeoTrust. So, all of these are examples of certification authorities, who would give you digital certificates.

Now, what are the main elements of a digital certificate? So, a digital certificate contains a lot of details such as, the certificate owner's identifying information, certificate owner's public key, dates between which a certificate is valid. So, it will give a from-date and a to-date during which the certificate is valid.

And once the validity is over, the certificate again has to be renewed and of course, the serial number of the certificate and digital signature of the certificate issuer. So, these are some of the details. There are also some other details such as hash algorithm and a lot of other details that you can see in a certificate.

(Refer Slide Time: 13:52)



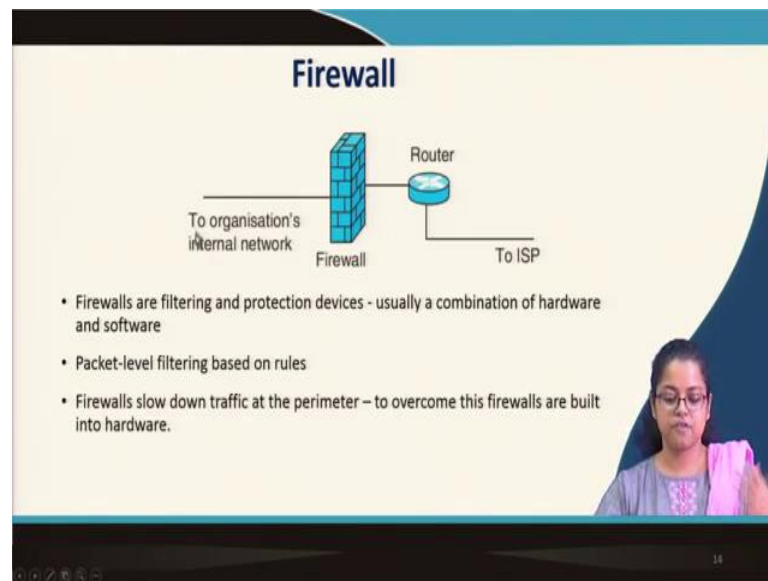
So, digital certificates usually look like this. I am not sure if you have actually gone ahead and seen a digital certificate for yourself. So, let me spend a couple of minutes on what a digital certificate looks like.

So, if you go to SBI; say SBI is a very popular bank in the Indian context. And if you go to the bank SBI or any other you know website which stores confidential information of customers, you would see a small green lock. So, on the where the website URL is there. So, once you click on that lock, you can see the digital certificate.

So, digital certificate looks like this; here, you have details about the certificate such as it is issued to SBI, it is issued by a popular certification authority digits DigiCert Global and it is valid from this date to this date. So, once this date you know this is over, then it has to be renewed. Now, the next. So, here there are some other so details and certification path, if you click on details, you would see details about the digital certificate such as we have mentioned all of these in the previous slide.

So, you would see a serial number, you would see a signature algorithm, a signature hash algorithm, issuer details, validity details; so, valid from valid to, who is the subject here you can see, the details about the subject and public key and several other details are also there, but these are the most prominent detail; details present in the digital certificate. So, this is what it looks like.

(Refer Slide Time: 15:47)



Now, moving on from digital certificates firewall. What is a Firewall? This is you know. So, far, we have been talking about different technology solutions to security breaches. So, a firewall is a network security solution to a security breach. So, what is a firewall? A firewall has, so here you see this is the firewall and this is the exterior. So, this is external to the organization. It goes to the internet service provider through the internet service provider to the internet and here we see, it goes to the organization's internal network right.

So, the firewall is the major line of defense here. Firewalls are filtering and protective devices, usually a combination of hardware and software. So, firewalls are filtering devices and protection devices; usually they are a combination of both hardware and software.

Firewalls are; you know, how do the firewalls work? So, firewalls perform packet level filtering based on certain rules. So, when data comes through the routers in the form of

packets, there are security policy rules based in the policies of these firewalls. So, firewalls have their own policies, wherein there are certain rules.

Now, these rules would say, you know, they would filter out or not allow packets coming from certain data sources to enter into the organization's interior. So, rules could be based on say you know websites which would not be you know data sources from those websites, data packets would not be allowed to enter the network or maybe data packets from certain IP addresses would not be allowed into the network.

So, there could be multiple rules that are that are you know coded into the security policies of these firewalls so that based on those rules data sources or data packets from those data sources are not allowed into the network.

If you want, if you do not want your you know you know suppose here there is an organisation and if the organisation does not want social media you know data packets from social media websites to and penetrate the firewall and then, come into the organisation; because it finds out that organisation employees are spending a lot of time on social media.

So, they can craft certain policies or rules into the firewall software stating that some of these you know some of these entities, some of these data packets from the social media websites do not are do not enter the organisations interior and they are stopped or filtered out at the firewall itself. Now, there is a flip side to firewalls. Firewalls slow down the traffic at the perimeter. So, that is a problem to firewalls because they slow down the traffic at the perimeter.

To overcome this problem firewalls are built into hardware because if firewalls are built into software, they have to go through each rule and they have to filter based on each rule. So, what may happen is they can take a lot of time and they can slow down the traffic at the perimeter. To overcome this problem, many a times, firewalls are built into hardware. So, this is how overall a firewall works.

(Refer Slide Time: 19:25)

Virtual Private Network (VPN)

- A technology that enables clients or employees of an organisation, who are outside the network, to connect securely to the organisation on the public Internet.
- It creates a 'tunnel' relying on authentication and encryption.

The diagram illustrates a Remote-access VPN setup. On the left, a laptop labeled 'Client Software' is shown at a 'REMOTE LOCATION'. A green line labeled 'Secure VPN Connection' extends from the laptop through a cloud labeled 'INTERNET' to a 'Network Access Server (NAS)' at the 'MAIN OFFICE'. The NAS is connected to a server rack representing the office network.

Now, coming to the next category of again this is a network security solution. So, this network security solution is called a Virtual Private Network. So, what is a virtual private network? This is a technology that enables clients or employees of an organisation, who are outside the network to connect securely to the organisation on the public internet.

So, it may so happen that there is an organisation or maybe a school or maybe a university and there are some students and professors, who are residing within the campus. So, those who are residing within the campus are automatically able to access internal websites, the intranet the ERP which is hosted on premise.

So, they are able to access all of these because they are within the organisations or institutes network. But there are certain employees, staff, students, maybe students go on vacation, they would want to access the internal organisation, the institutes internal resources, they would want to access the ERP, they would want to access the you know intranet.

So, they would want to access all of these from outside and there are also certain employees, who commute every day from outside the institute. So, they would also want to access the institutes services from outside. So, for that a VPN, plays a very important role. A VPN creates a tunnel relying on authentication and encryption and this tunnel

ensures that the communication between the remote location, where the client software is located and the main office habits extremely in a secured manner.

So, the connection which is through the internet, if it happens through the VPN or the virtual private network, it cannot be intercepted by third parties and it is extremely secure. So, VPN is a network security solution, which is aimed at enhancing the security of in of communications between for individuals who are residing outside institute premises.

Otherwise, if that you know tunnel is breached, through that breach the hackers can penetrate into the institute or the organisations internal network and can then wreak havoc. So, VPN is a very-very important network security solution.

(Refer Slide Time: 22:04)



Now, moving on, we had discussed about phishing attacks in the previous in this session itself, we have begun with phishing attack. So, let us end with counter measures to phishing attacks. The primary countermeasure to phishing attack is awareness, very-very critical. So, phishing you know phishers are very innovative, they can come up with very crafty, new innovative kind of e-mails and if a common user or a customer of a particular website is not familiar with what a phishing attack is, it is very easy for the user to fall prey to the phishing attack.

So, therefore, as I mentioned at the beginning of this session, banks because banking websites are extremely susceptible to phishing attacks. So, banks always alert their customers about phishing attacks and problems that could happen with phishing attacks, problems that could happen if a customer falls or prey to phishing attacks and divulges his or her information.

So, most important step that a company can take today against phishing attacks is to educate website users. Many companies contract consulting firms that specialize in anti-phishing filters. So, there are also anti phishing filters which are which play a very important role because these filters are you know based on machine learning. These filters are created such that based on prior data, you know they create certain you can say certain patterns.

And if a particular phishing e-mail follows any of those patterns, it is very easily classified as a phishing e-mail and it is not allowed to enter into the user's mail box. However, as we said that phishers are also very-very, you know, these days phishers are very intelligent; phishers come up with more unique and out of the box e-mails.

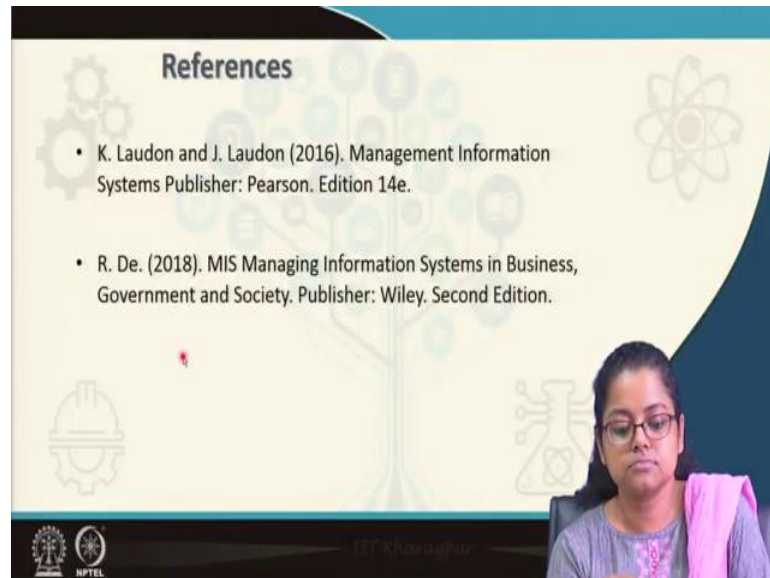
So, the e-mails are drafted in such a, such an unique format that even if the phisher, if the anti-phishing filters are not updated constantly, they may not be able to classify a particular e-mail as a phishing e-mail based on the prior data. So, in that case the phishing e-mail would not be classified as a phishing e-mail and it will enter the phishers, the users mail box and the user if he or she is not alert, then the user can fall prey.

Now, therefore, it is very important to dedicate time and effort to come up with dynamic anti-phishing filters. And the last counter measure is of course, reporting phishing e-mails. This is important, if you have actually encountered a phishing e-mail, it is you can report it there are a lot of websites to which you can report anti-phishing to which you can report phishing e-mails.

This is one example of a website where phishing e-mails can be reported. So, such websites do have a huge repository of phishing e-mails and these data from these websites are constantly used to develop more dynamic anti-phishing filters. So, if you are experiencing a phishing e-mail in your mail box, please report it to some of these anti phishing, you know, filters' databases or you can report it to some of these websites from

where data will be used to improve upon the anti-phishing filters that exist; right. So, these are some of the countermeasures to phishing attacks.

(Refer Slide Time: 26:02)



So, today we have discussed some of the countermeasures to the different kinds of attacks that are there. In the next session, we will talk about some other countermeasures to information security breaches; technical countermeasures also, we will discuss a few. And then, we will move on to organizational and legal countermeasures that can be taken to protect information system, information security breaches in organizations.

So, with that we come to the end of this session and hope to see you in the next session!

Thank you!