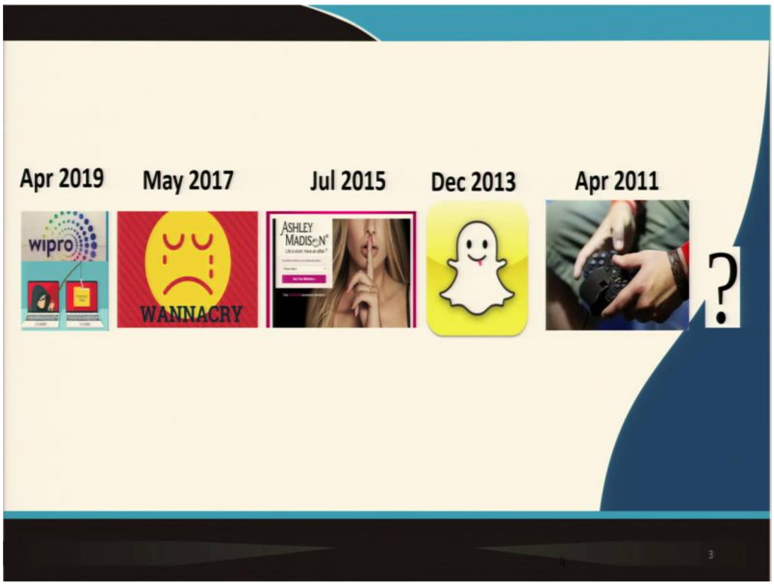
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module -11
Ethical, Social and Security Issues in MIS
Lecture - 53
Security Issues in MIS – I

(Refer Slide Time: 00:12)



Hello, welcome to this module 11, session 3! So, in this session rather in this module, we are talking about 'Ethical, Social and Security Issues' with respect to Management Information Systems.

So, in the previous two lectures we had spoken about predominantly ethical and social issues with respect to MIS, issues such as we had spoken about privacy, piracy etcetera. In this session, we will focus on the Security Issues with respect to MIS. So, let us proceed with this session.

So, you can see here there are five you know pictures and there are some dates associated with those and then there is a question mark; so, does it ring a bell? Alright. So, we are talking about a very high profile information security breaches that have happened across the world.

Now, if we begin here the issues or the information security breaches are displayed in chronological order. So, it starts with April 2011, the next incident happened in December 2013, followed by July 2015, then May 2017 and finally, the one that we wanted to highlight the latest security breach here in April 2019.

So, all of these breaches happened on very large high profile companies and exposed how vulnerable the companies are. Let us spend a couple of minutes on each of them; the first one here April 2019. So, it is the most recent breach; its if you see here it is the breach happened on Wipro which is an information technology services company in Indian context.

And the kind of attack here was a very serious kind of phishing attack that happened and this attack exposed a lot of customers, it exploited the information of a lot of customers of this very high profile IT Company in the Indian context.

The next one I think is very-very, is a very-very notorious cyber breach that happened in May 2017 and it devastated, you know, several companies, offices, hospitals across the entire world. It was the ransomware attack known as Wannacry; so, this breach actually tormented a lot of individuals, a lot of businesses and had a huge financial impact.

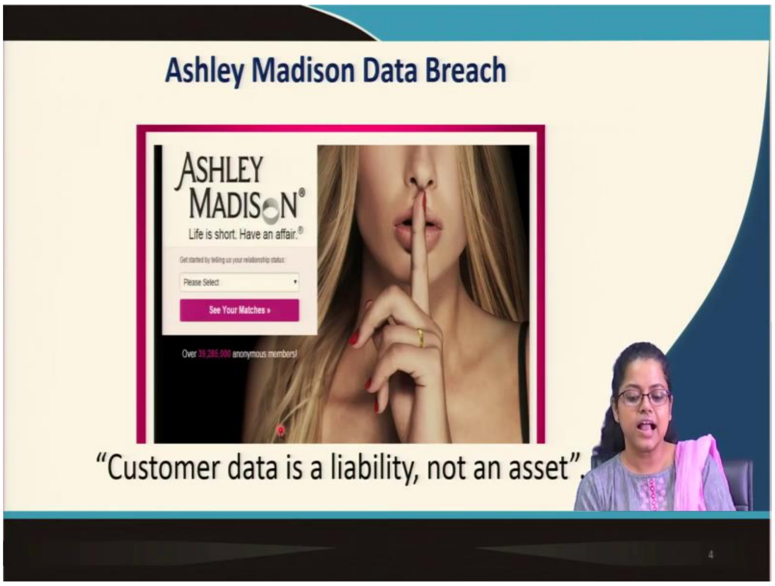
The next one in July 2015 was on a company named Ashley Medicine. So, those of you who are not familiar with this company; it is a company it is an e-commerce company which is the logo of which is you know or the tagline is life is short; have an affair. So, it is a website for having extramarital affairs.

Now, what happened is this particular company was breached in 2015 and a lot of confidential information, including a lot of you know customer IDs of people who were members of this particular ID were exposed. The next one that we want to highlight here is a breach on your favorite you know; maybe we can call it a messenger or we can call it a chat platform known as Snap chat.

So, in December 2013 Snapchat was hacked and the user IDs, passwords and a lot of other confidential information of customers or users were revealed in public. And the latest; last one here April 2011 was, as you can see a cyber breach on Sony PlayStation. So, users of Sony PlayStation across the world were exploited; their information was stolen and there was a huge financial impact of this breach as well.

So, all of these incidents reflect how critical, how severe information security breaches can be for information systems of organizations. So, with that context let us move on.

(Refer Slide Time: 05:05)



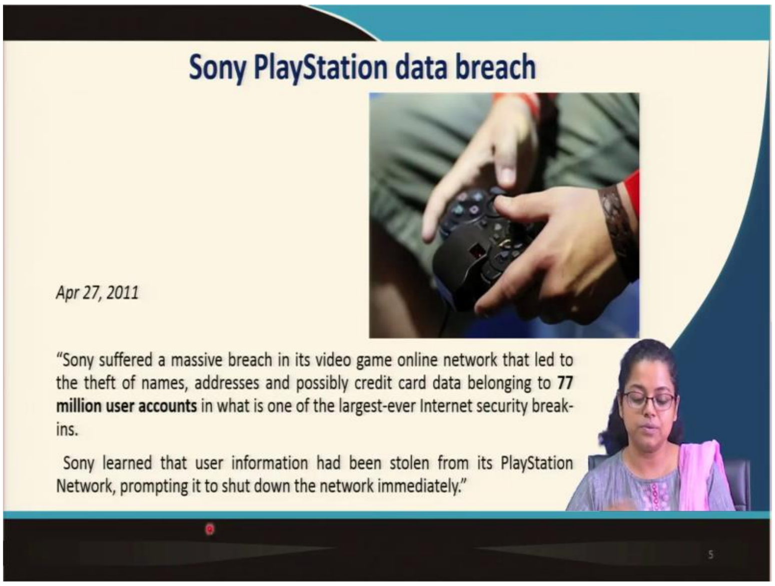
Ashley Madison Data Breach

“Customer data is a liability, not an asset”.

Let us spend a few minutes again on each of these. So, the Ashley medicine data breach as we had we have just spoken about it some time back, revealed the fact that customer data is a liability and not an asset because if you have customer data as a company, you are supposed to safeguard that data.

So, it is a liability because in case something untoward you know untowardly happens with that kind of data; it is going to hamper the reputation of your company. So, it is not an asset, but it should always be treated as a liability.

(Refer Slide Time: 05:44)



Sony PlayStation data breach

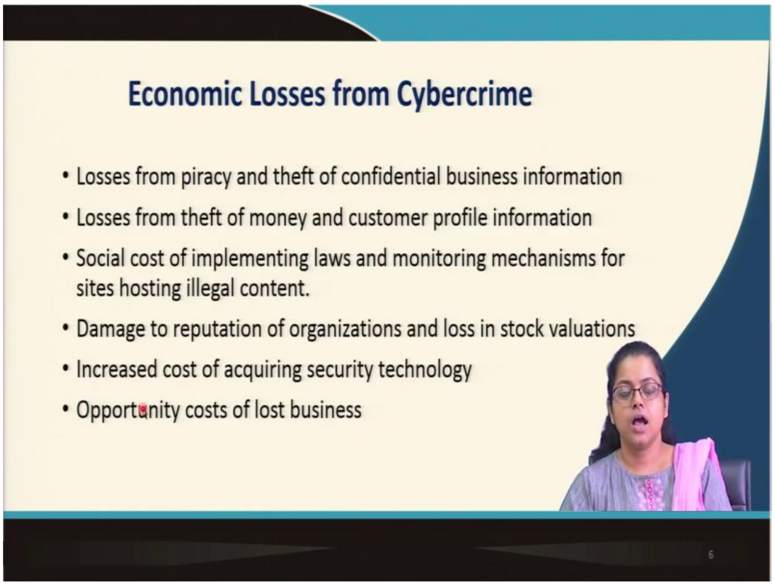
Apr 27, 2011

"Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to **77 million user accounts** in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network, prompting it to shut down the network immediately."

The next one again the Sony PlayStation breach; Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts which is one of the largest ever internet security break ins. So, you can understand; 70 million user accounts at stake.

(Refer Slide Time: 06:10)



Economic Losses from Cybercrime

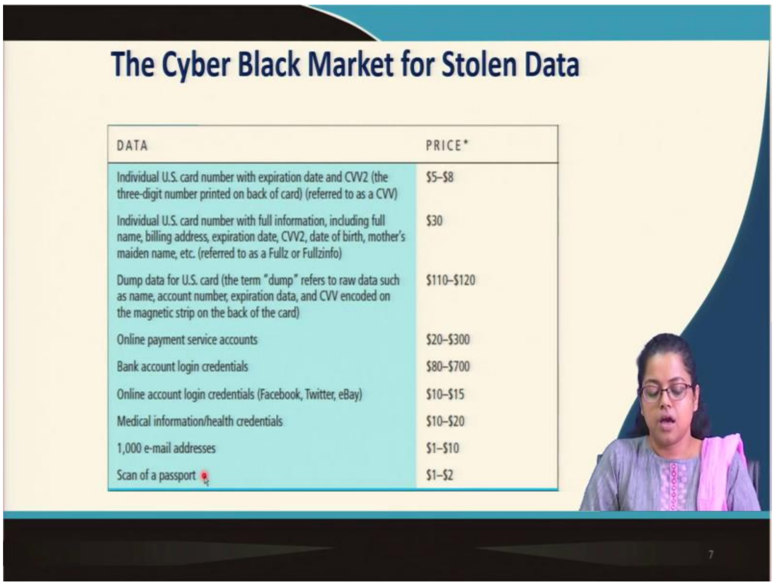
- Losses from piracy and theft of confidential business information
- Losses from theft of money and customer profile information
- Social cost of implementing laws and monitoring mechanisms for sites hosting illegal content.
- Damage to reputation of organizations and loss in stock valuations
- Increased cost of acquiring security technology
- Opportunity costs of lost business

Now, coming to economic losses from cyber crime; losses from piracy and theft of confidential business information, losses from theft of money and customer profile information. So, social cost of implementing laws and monitoring mechanisms for sites hosting illegal content, this also, you know, adds to economic losses from cyber crime.

The next loss pertains to damages to reputation of organizations and loss in stock valuation. This is a very significant you know damage that happens because it is it has been observed through research that companies lose substantial amount of their value in terms of the stock market valuation of companies once a cyber breach on the company is disclosed.

The next one increased cost of acquiring security technology because if you have suffered a cyber breach; you would have to go ahead and implement a lot of security technologies in the future. And the last one, opportunity cost of lost businesses, of course, this is again very-very critical. So, all of these describe the economic losses that companies can undergo as a result of cyber breaches on them.

(Refer Slide Time: 07:37)



The Cyber Black Market for Stolen Data

DATA	PRICE*
Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV)	$5–$8
Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo)	$30
Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card)	$110–$120
Online payment service accounts	$20–$300
Bank account login credentials	$80–$700
Online account login credentials (Facebook, Twitter, eBay)	$10–$15
Medical information/health credentials	$10–$20
1,000 e-mail addresses	$1–$10
Scan of a passport	$1–$2

7

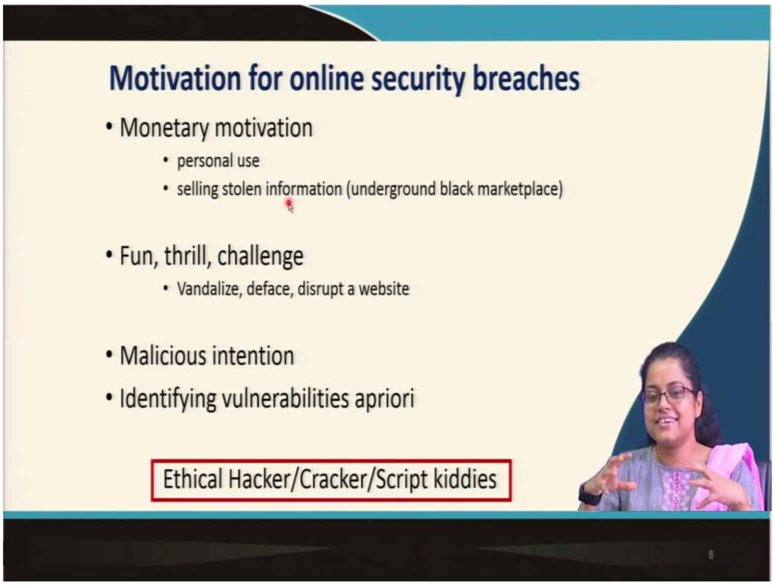
Now, moving on; this data has been obtained from one of the references that I have mentioned at the back of this slide; so, by from the book by Laudon and Laudon. So, this mentions that there is a huge cyber black market for stolen data and you know different categories of data have different prices in the cyber black market which is a very we have heard of underground we have heard of black market, but we have we ever heard of or thought about the cyber black market for stolen data, this presents a very-very grim situation.

So, you would see here that different categories of data such as bank account login details. The price in the cyber black market is around it ranges from 80 dollars to 700 dollars, it is that huge. Similarly, you know a 1000 email addresses; if they are stolen and if they are sold in the cyber black market, it costs around 1 to 10 US dollars.

So, then you would see here that online payment service accounts would the price is around 200 dollars to 20 dollars to 300 dollars. Similarly, medical information or critical health credentials; the price is around 10 to 20 US dollars. So, for every category of data; there is a rough price that is quoted here. So, this is the price at which you know data pertaining to these categories are sold in the cyber black market.

So, data is not only stolen from customers and you know users of platforms; data is also sold. So, you never know where your data is going, if it is once stolen from the repositories of the companies whom you trust so much. So, that presents how severe cyber security and of course, information security is for organizations; especially with the arrival of information systems.

(Refer Slide Time: 09:42)



Motivation for online security breaches

- Monetary motivation
  - personal use
  - selling stolen information (underground black marketplace)
- Fun, thrill, challenge
  - Vandalize, deface, disrupt a website
- Malicious intention
- Identifying vulnerabilities apriori

Ethical Hacker/Cracker/Script kiddies

Now, moving on; we have seen that you know breaches and different categories of data that are stolen have their own prices. So, what are the motivations, what motivates people or group of people to perform online security breaches?

The primary motivation is monetary in nature. So, a lot of people use it for personal gains, personal financial gains of course, and some people as we have just discussed sell it in the cyber black market um. So, that is the monetary motivation for cyber breaches or online security breaches. Along with this, with it, there is another very-very important motivation and that is fun, thrill or challenge.

So, a lot of people would like to perform security breaches on high profile companies or say government websites just because they take it up as a challenge or they find you know some sort of inherent thrill or fun in breaking into the system and maybe defacing a website or maybe stealing some data. So, fun, thrill and challenge is another motivation for security breaches.

The third motivation that we would want to highlight is of course, the most dangerous and it has to do with malicious intention. So, if a lot of companies are actually hacked because the hacker has a malicious intention in mind. So, let us take an example say you are a very popular player in your particular domain, you are a very popular company and you do have a lot of competitors.

Your competitors are not be not able to get ahead of you by you know ethical means; so they resort to some malicious you know activities in order to tamper your reputation. So, they can actually launch some sort of cyber breach on you so that they can steal your data or they can, you know, tamper with your, you know, with your image in public which would actually take a huge hit on your reputation. So, many companies or many hackers do have a malicious intention in mind.

So, based on these motivations that we have just discussed monetary, thrill, challenge or a malicious intention you know cyber breaches or the hackers of cyber breaches are categorized into three categories. The fourth intention which I have not mentioned so far is identifying vulnerabilities apriori. So, of course, the first three intentions are motivations that we have discussed so far are not so positive in nature, they are they are kind of negative in nature.

The fourth one of course, are identifying vulnerabilities apriori; it is generally you know used by hackers who do it for a good intent. So, they are in general appointed by companies, so that they can identify vulnerabilities or loop holes in those companies information systems apriori that is even before they are breached, so that you know once the vulnerabilities are identified they can be patched or certain measures can be taken to protect them from future breaches.

So, the fourth intention that we or the motivation that we speak here for an online security breach is of course, very benign and very you know positive in nature. So, based on these four motivations; of course, the first three are not for, not positive motivations the last one is a positive motivation.

So, based on these; the hackers can be or maybe yeah hackers can be categorized into three categories. The first one ethical hacker; so ethical hackers are those who are; for whom the motivation is the fourth one here. So, those who try to get into a system in order to in order to identify vulnerabilities or loop holes apriori, but they do not have any malicious intent in mind; what they want to do is inform the organization that you do have these problems, so you have to take care of them before your system is actually breached.

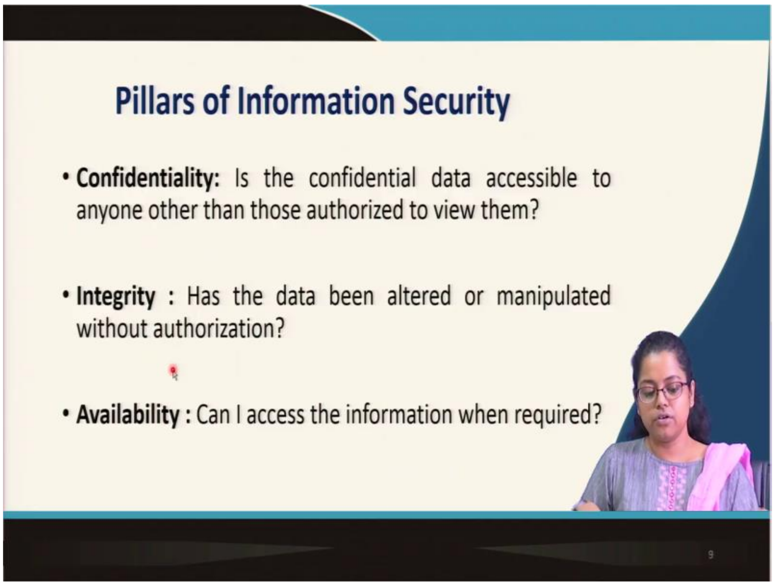
The second one here cracker; crackers are those hackers who are who have a malicious intention. So, those with the fourth and also the first kind of intention and to an extent even the second one. So, those with the malicious intention in mind are considered as crackers.

And the third one script kiddies; so as the name suggests script kiddies are those who are you know they are not a very sophisticated hackers, they do not have the expertise to go ahead and hack, but what they can do is; they can maybe run some scripts that are available online, they can run them and they generally hack for fun, thrill or challenge here.

So, in general script kiddies are maybe college students or students who are familiar with technology, but do not do not have the expertise to perform a high profile breach on their own. What they would do is they would rely on some readily available scripts online and they would take them run them and then use them for hacking systems or maybe you know defacing a website.

So, generally there the outcome of their breach is not very severe; what they do is they can actually, they can vandalize, deface or disrupt a website for the fun, thrill or challenge of it but in general they do not have a malicious intention in mind. So, these are the motivations of security breaches and the categorization of hackers based on these motivations.

(Refer Slide Time: 15:52)



Pillars of Information Security

- **Confidentiality:** Is the confidential data accessible to anyone other than those authorized to view them?
- **Integrity :** Has the data been altered or manipulated without authorization?
- **Availability :** Can I access the information when required?

Moving on pillars of information security; so, any discussion information security would be; would not be able to would be futile in nature, if we do not discuss the three very important pillars of information security. The first pillar is known as confidentiality of information. So, is the confidential data accessible to anyone other than those authorized to view them?

So, what this means is this the first pillar of information security, this means that data in order to be considered secure should be very confidential or the confidentiality should be maintained which means that in other words, only those who are authorized to view them or maybe you know alter them or modify them or work with them only those authorized entities should be able to access the data; not the rest, unauthorized entities should not be able to access the data at any cost.

The second pillar very important has to do with integrity of data which means that has the data been altered or manipulated without authorization? So, if in case you know somebody who is not authorized to handle your data, gets access and can also alter or manipulate of your data. Confidentiality has to do with those who have the power to view data and integrity has to do with those who have the power to alter or manipulate data those who are unauthorized, but have been able to alter or manipulate data. So, that should not be possible at any cost, only then the integrity of data would be maintained.

And the third pillar deals pertains to availability of data. So, this is something that we generally do not perceive when we talk about information security. But availability is another very-very important pillar of information security; what this means is the data available whenever I require it, so, can I access the data or the information whenever I require it; let me give you some examples.

So, availability becomes very important in case of say healthcare information system. So, if the healthcare information system maintains electronic medical records or electronic health records of patients and say you know that data from that particular database has to be fetched during an operation of a patient and at that point in time the data is suddenly not available. So, that can result that can result in a huge disaster, it can even cost the life of the patient.

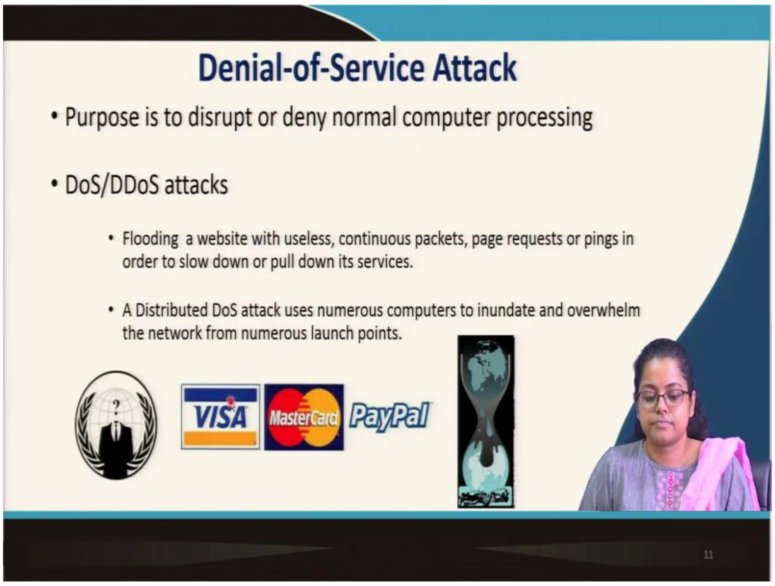
So, availability of data is extremely important and it is the third most important pillar of information security; especially during times when they should actually be available. So, the site should not be down, the database should not be inaccessible when I actually need the data. So, these are the three important pillars and in short; they are considered they are you know you would hear people mentioning CIA of data; so that means confidentiality, integrity and availability of data.

(Refer Slide Time: 19:08)

Security Threats in Organizations

Moving on, security threats in organizations; so, let us talk about some of these security threats.

(Refer Slide Time: 19:15)



Denial-of-Service Attack

- Purpose is to disrupt or deny normal computer processing
- DoS/DDoS attacks
  - Flooding a website with useless, continuous packets, page requests or pings in order to slow down or pull down its services.
  - A Distributed DoS attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

The first one here; denial of service attack, so as the name suggests denial of service attack. The purpose of this kind of attack is to disrupt or deny normal computer processing. Denial of service attack or distributed denial of service attack. So, let us see how what is the difference between the two.

DoS attack in short that is Denial of Service attack means flooding a website with useless continuous packets, page requests or pings in order to slow down or pull down its services. So, in order to bring down the website; it is flooded with a lot of useless continuous packets, page requests or pings so that the site, so that the entire bandwidth gets choked and the site goes down. So, that is considered to be a denial of service attack and it has a variant which is distributed denial of service attack.

Distributed denial of service attack uses numerous computers to inundate and overwhelm the network from numerous launch points. So, this means that the attack to your website does not happen only from one particular you know malicious entity or a hacker or a malicious source, but it happens from multiple sources or multiple computers, who send a large number of requests or pings or you know packets of data so that your entire network gets choked right. So, this is the difference between DoS and DDoS attack.

So, there are a lot of examples of DoS attacks that have happened in the past. But here I would want to you know highlight a very interesting example of a DDoS attack that happened. And here we have you know this is one logo of some of a group of people, this is another logo that we are talking about and this is the third.

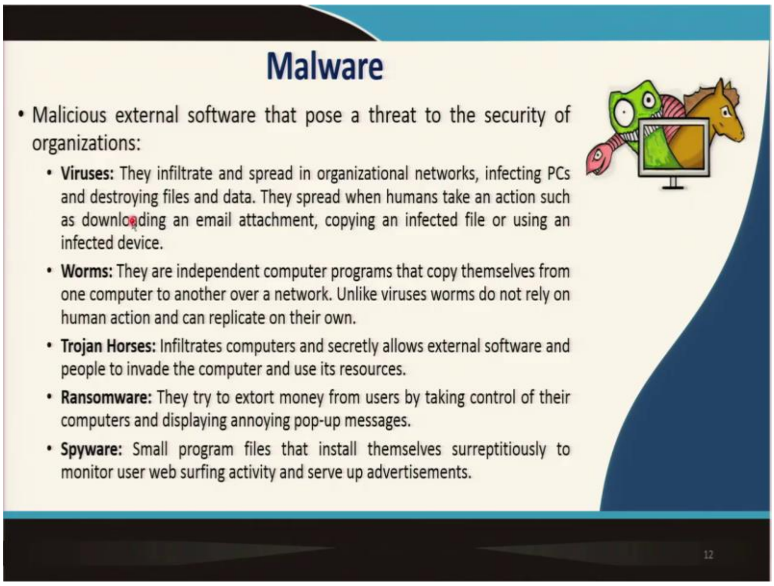
So, I would want ideally you to be able to connect the dots, but then let me tell you how these three graphics here are related to a denial of service attack. So, this; so in 2011; this the first one here, the first logo stands for anonymous group of hacktivists. So, here is the term hacktivist; what does that mean? It is a it we are combining two terms here hackers and activists and together we have a term called hacktivists.

So, who are these hacktivists? Hacktivists are those activists who hack in order to protest and this; these group; this group of hacktivists are known as the anonymous group of hacktivists. So, they hack in order to protest for good causes. Now, the second group of you know logos here of course, I am sure you are you all are familiar with them. So, these are you know visa MasterCard and PayPal; so they are in general players in payment processing right.

And the third one very very interesting; it represents Wikileaks right. So, now, what happened is or how these three are connected to each other is; in 2011 anonymous group of hacktivists launched a denial of a; distributed denial of service attack on all of these players in payment processing because they wanted to protest and they always protest for good causes. So, they wanted to protest because these players in payment processing were not willing to process the donations that were going to Wikileaks.

So, this is how three of these you know entities here that have demonstrated through the logos are connected by an overarching denial of service attack or distributed denial of service attack. So, this is how these are connected to each other. Now, moving on this is the first category of information security threat.

(Refer Slide Time: 23:27)



Malware

- Malicious external software that pose a threat to the security of organizations:
  - **Viruses:** They infiltrate and spread in organizational networks, infecting PCs and destroying files and data. They spread when humans take an action such as downloading an email attachment, copying an infected file or using an infected device.
  - **Worms:** They are independent computer programs that copy themselves from one computer to another over a network. Unlike viruses worms do not rely on human action and can replicate on their own.
  - **Trojan Horses:** Infiltrates computers and secretly allows external software and people to invade the computer and use its resources.
  - **Ransomware:** They try to extort money from users by taking control of their computers and displaying annoying pop-up messages.
  - **Spyware:** Small program files that install themselves surreptitiously to monitor user web surfing activity and serve up advertisements.

12

The next one malwares; so malwares if you see here; malicious external software that pose a threat to the security of organizations; so, there are here we have mentioned five categories of malwares. The first one viruses, viruses infiltrate and spread in organizational networks infecting PCs and destroying files and data.

Of course, viruses spread when human beings take an action; such as if you are downloading an email attachment which is infected or copying an infected file or may be inserting an infected device into your system infected device such as a USB drive, any infected device if you are inserting into your system that could result in you know transmission of a virus to your system.

So, there are a lot of popular viruses and I think I am not sure if there is anybody around you know watching this video or taking up this course who has not experienced a virus threat in his or her life. So, you know one popular; so I love you virus was very very popular in 2000, I suppose in the year 2000 and it wrecked havoc.

The next one worms; worms are very similar to viruses, but there is a very subtle difference. So, worms are independent computer programs that copy themselves from one computer to another over the network. Unlike, viruses which require human intervention in order to spread, worms do not rely on human intervention or action and they can replicate on their own.

So, worms replicate on their own therefore, worms are often considered to be much more malicious compared to viruses and they actually cause greater damage than viruses. Some popular worms that I can remember are the conficker worm, my doom worm; so all of these actually created a lot of havoc in systems.

The third one that I want to highlight is the Trojan horse; so Trojan horse infiltrates computers and secretly allows external software and people to invade the computer and use its resources. So, they are very similar to viruses, but they are kind of docile and kind of dormant in nature.

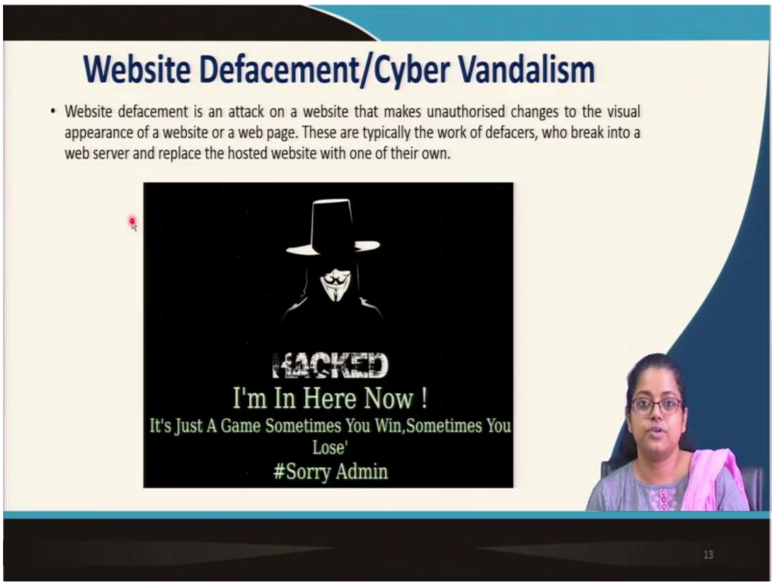
But, then similar to the mythological Trojan horse which was used in Greek mythology; Trojan horses actually are very dangerous because though they appear to be very dormant; what they do is they can secretly allow external software and agents to invade into a computer and then create a problem there. On their own, they will not create any problem, but they will you know create a loop hole or an entry point for some third party, some other computer program to come into the system and create a damage alright.

So, the next one ransomware; we had spoken about the Wannacry ransomware breach that happened in 2017. And I am sure all of you were are familiar with the Wannacry and then there were a couple of others other ransomware breaches that happened.

So, ransomwares try to extort money from users by taking control of their computers and displaying annoying pop up messages. So, as the name suggests; they would want to ransom if you they would ask a ransom from you by taking control of your computer and unless you pay the ransom, they would not release your system.

And the last one spyware, we have discussed it in the previous lecture on privacy. So, there we were saying that spywares are small computer files that install themselves surreptitiously into your system to monitor user web serving activity and serve up advertisements. So, they are very-very dangerous; we had discussed it before why; alright.

(Refer Slide Time: 27:48)



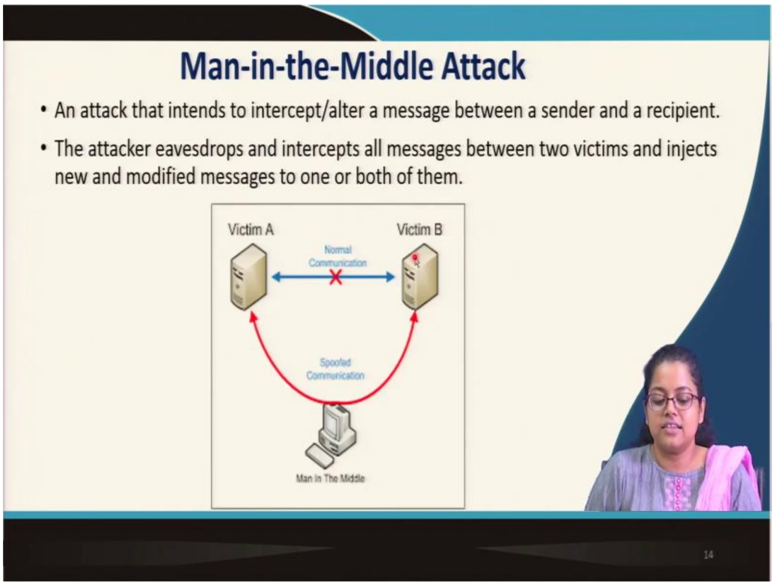
Website Defacement/Cyber Vandalism

- Website defacement is an attack on a website that makes unauthorised changes to the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.

So, we move on from malware to the, you know, next category of cyber breaches now which are to do with website defacement or cyber vandalism. Website defacement is an attack on a website that makes unauthorized changes to the visual appearance of a website or a web page. These are typically the work of defacers of course, and we had mentioned that websites are generally defaced by people who or hackers, who want to do it for thrill or challenge or fun.

So, defacers who break into a web server and replace the hosted website with one of their own; so, often you would see a lot of government websites being defaced by their neighbors just because of they can the neighbors consider it to be a challenge. So, a defaced website may look like this. So, your website would be replaced by the by some texts and some images showing that you know how vulnerable you are. So, this is about cyber vandalism.

(Refer Slide Time: 28:57)



Man-in-the-Middle Attack

- An attack that intends to intercept/alter a message between a sender and a recipient.
- The attacker eavesdrops and intercepts all messages between two victims and injects new and modified messages to one or both of them.

And the next attack or the next security breach that we want to highlight is about the man in the middle attack. So, this is again a very very severe kind of breach because this is an attack that intends to intercept or alter a message between a sender and a recipient.

So, if you have a sender and a recipient here both of which who would eventually become victims; an attacker eavesdrops and intercepts all messages between two victims. So, here is an attacker; a man in the middle who would eavesdrop and disrupt the normal communication, he would intercept the normal communication and inject new and modified messages to one or both of them.

So, instead of the normal communication that was happening between victim A and victim B; now there would be there is a man in the middle. So, the man in the middle you know eavesdrops and interjects the original message and tampers it, manipulates it or maybe alters it to send a different message altogether to either or both of the victims. So, this is a man in the middle attack and it is also kind of very-very dangerous breach.

(Refer Slide Time: 30:12)

References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.
- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

So, I think with this we come to the end of this session, we have discussed some; we have begun discussing about some of the different categories of security threats that are there in the world of information system.

In the next lecture or next session, we will talk about some other very-very relevant, very important security breaches and then, we will try to see about the counter measures to or the solutions to these security breaches; alright.

Thank you and see you in the next session!