



NPTEL ONLINE CERTIFICATION COURSES

Management Information System

Saini Das

Vinod Gupta School of Management, IIT Kharagpur

Module 11: Ethical, Social and Security issues in MIS
Ethical and Social Issues in MIS - I

Ethical and Social Issues in MIS

- Ethics refers to the principles of right and wrong that individuals use to make choices to guide their behaviour.
- Information Systems (IS) raise new ethical questions because they provide opportunities for intense social change, and thus threaten existing distributions of money, power, rights and obligations.
- Ethical issues in IS have been amplified by the rise of Internet that makes it easier to assemble, integrate and distribute information.
- Some of important ethical and social issues in IS are:
 - Information Privacy Issues
 - Intellectual Property Rights Infringement
 - Workplace Monitoring

Ethical Issue : Privacy



“The right to be left alone and the right to be free of unreasonable personal intrusions”.

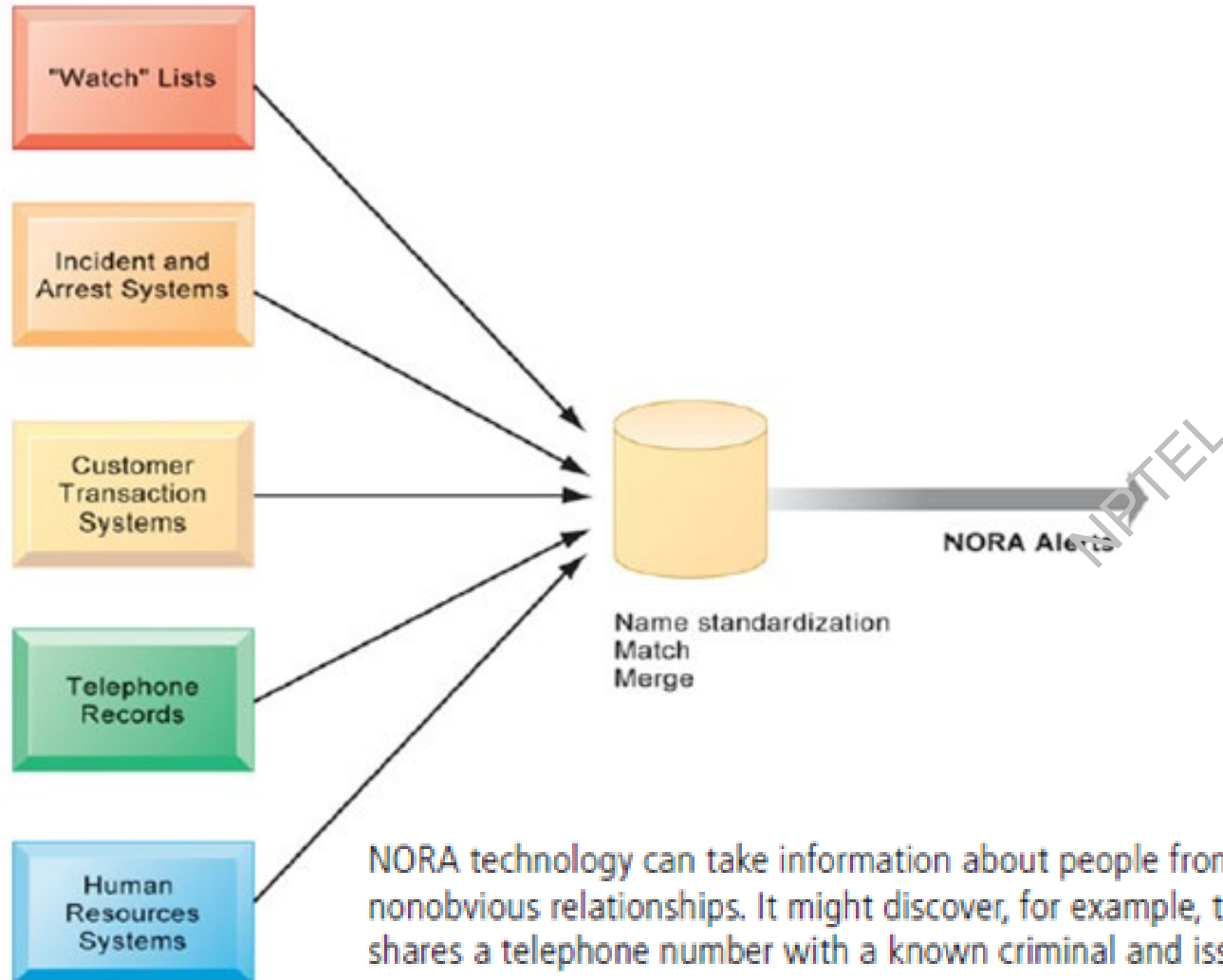
- The right of privacy is not absolute. Privacy must be balanced against needs of society.
- The public's right to know is superior to individuals' right to privacy

Key terminologies

- **Profiling:** The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals.



NORA



NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

Information Collected on the Internet

- **Personally identifiable information (PII)**

Name	Gender	Education
Address	Age	Preference data
Phone number	Occupation	Transaction data
E-mail address	Location	Clickstream data
Social security number	Location history	Device used for access
Bank accounts	Likes	Browser type
Credit card accounts	Photograph	

- **Anonymous information**

- Age; occupation; income; zip code; ethnicity

Mechanisms to collect information about individuals on the Internet

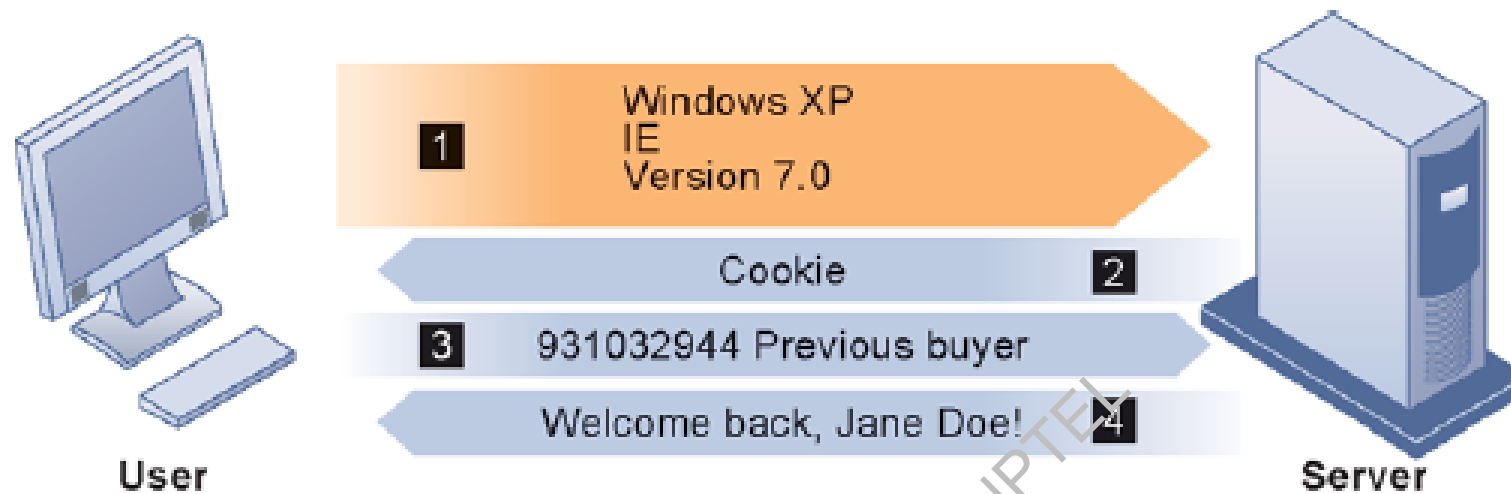
- Web Site Registration
- Cookies
- Web Beacons
- Spyware

NPTEL

Cookies

- Cookies are small text files deposited on a computer hard drive when a user visits websites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie depending on the activity during the visit.

How cookies identify visitors?



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

Web Beacons

- Web beacons, also called Web bugs, are tiny objects invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending an e-mail.
- Web beacons are placed on popular websites by “third party” firms who pay the Web sites a fee for access to their audience. Typical popular Web sites contain 25–35 web beacons.

Spyware

- **Spyware** is a software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- Spyware can collect almost any type of data, including personal information like internet surfing habits, user logins, and bank or credit account information.
- Spyware can also interfere with user control of a computer by installing additional software.
- Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.



Technical Solutions

- Anti-spyware technologies
- Email encryption
- Do Not Track options
- Opt-out model of informed consent
- Opt-in model of informed consent
- Making email or surfing anonymous

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.





**THANK
YOU !**



NPTEL ONLINE CERTIFICATION COURSES

Management Information System

Saini Das

Vinod Gupta School of Management, IIT Kharagpur

Module 11: Ethical, Social and Security issues in MIS
Ethical and Social Issues in MIS – II

Legal Solutions to Privacy Issues

- Laws
 - HIPAA
 - FIP
 - GDPR

NPTEL

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA of 1996 is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA.
- The Privacy Rule ensures that the privacy of individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care.



FTC's Fair Information Practices (FIP)

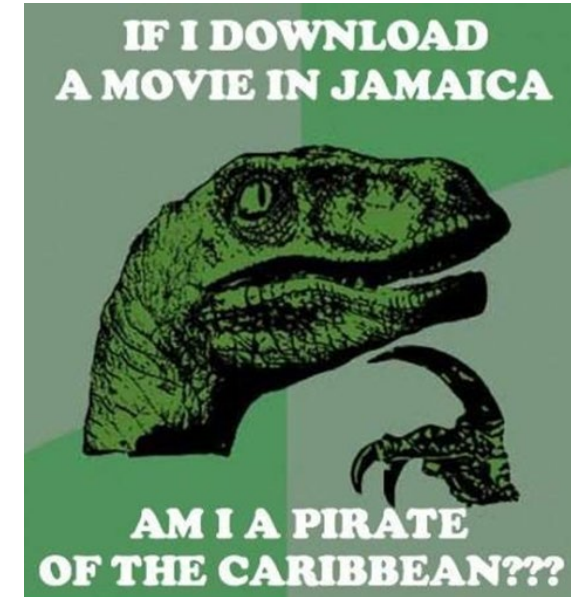
Notice/Awareness (core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data.
Choice/Consent (core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/opt-out clause must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be a mechanism to enforce the principles in place. This can involve self-regulation or legislation giving consumers legal remedies for violations.

General Data Protection Regulation (GDPR)

Purpose	<ul style="list-style-type: none">• Harmonize data privacy laws across Europe• Reshape the way organizations across the region approach data privacy.• Protect and empower EU citizens' data privacy
Scope	<ul style="list-style-type: none">• Applies to all firms and organizations worldwide that collect, process, or use personal information of EU citizens
Administration and enforcement	<ul style="list-style-type: none">• Creates a new EU-wide Information Commissioners Office to enforce the regulation in the European Union. Each country also has its own Data Protection Agency
Individual rights	<ul style="list-style-type: none">• Easier access to all personal data without charge within one month• Right to be forgotten (power to erase data)• Data portability: allow people to move their data to other providers• Give users more control over the use of their data by third parties and partners• Right to seek damages for abuse, including class action suits
Organizational requirements	<ul style="list-style-type: none">• Data protection officer in all firms with more than 250 employees, reporting to senior management• Requires explicit consent before collecting data on people (positive opt-in)• Published rationale for data collection and how long it will be held• Requires firms to report breaches, hacks, and unauthorized disclosure within 72 hours• Third-party risk management. Firms are liable for data shared with partners and must maintain a list of all sharing firms• Requires firms to maintain a record of all EU personal data• Privacy by design of all new systems• Targeting limits: allows anonymized data for audience targeting, but targeting based on social media or other personal profiles remains a grey area• New schedule of fines: up to \$20 million or 4% of global revenue• Privacy shield: agreements with non-EU countries to ensure any data processed outside the European Union meets EU GDPR standards

Ethical issue : Intellectual Property Rights Infringement

- Intellectual Property (IP) refer to creations of the mind, such as inventions, literary and artistic works, symbols, names, images, and designs, used in commerce.
- IT has made it difficult to protect intellectual property because computerized information can be easily copied or distributed on networks.
- IP is subject to a variety of protections under three different legal traditions:
 - Copyright
 - Trade Secrets
 - Patents



Copyright

- Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death.
 - Literary works
 - Musical works
 - Dramatic works
 - Artistic works
 - Sound recordings, films, broadcasts, cable programs
- Illegal file sharing services such as Kazaa, Napster, Torrent etc. help users share digital copyrighted software, music and video files.

Copyright Protection Approaches

- Legitimate online digital content stores and services such as, iTunes, Pandora, Kindle, Netflix have resulted in decline of some forms of piracy.
- Digital watermarks are unique identifiers embedded in digital content that make it possible to identify ownership or pirated works
- Digital Millennium Copyright Act 1998 makes it illegal to circumvent technology-based protections of copyrighted materials.
- Software and Information Industry Association (SIIA) runs an anti-piracy hotline for individuals to report piracy activities.



Trade Secrets



- Any intellectual work product – a formula, device, pattern or compilation of data used for a business purpose can be classified as a trade secret provided it is not based on information available in the public domain.
- Trade secret law protects the actual ideas in a work product.
- The creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

Patent



- A document that grants the holder exclusive rights to an invention for a fixed number of years (usually 20 years).
- Patent infringement occurs when another party makes, uses, or sells a patented item without the permission of the patent holder.
- The patent holder may choose to sue the infringing party to stop his or her activities, as well as to receive compensation for the unauthorized use.

Ethical Issue : Workplace Monitoring

- The need for monitoring has existed through the ages.
- Managements justify this need in two ways: to boost productivity – to ensure no 'free-loading' and to spot best performers and reward them; .
- Critique of monitoring – it is obtrusive, leads to lowered trust in the workforce, which lowers confidence.
- Pervasive use of information systems has increased the scale and precision of monitoring.

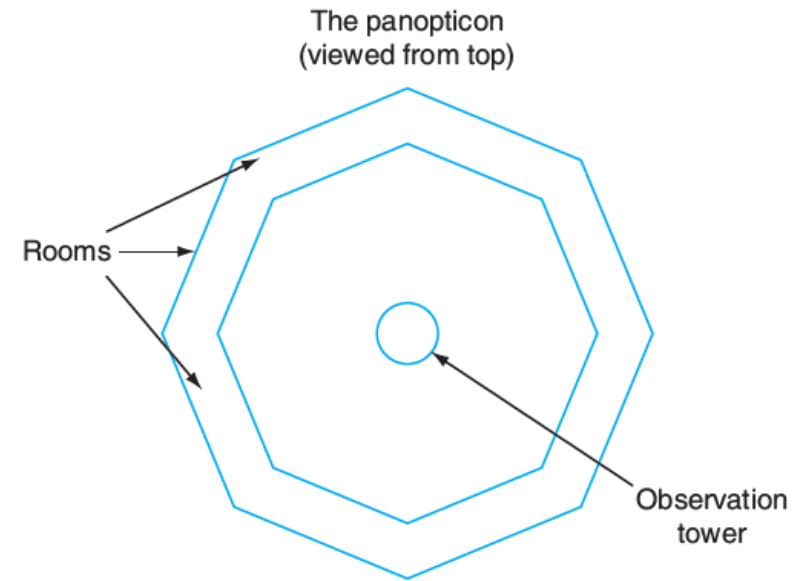


Workplace Monitoring: Use of Information System

- Use of digital video cameras
- Use of computer network logs
- Scanning and storage of outgoing and incoming emails
- Use of employee identity cards to monitor physical movements
- Access to all files on employees' personal computers and laptops

Information Panopticon

- Conceived by British economist-philosopher Jeremy Bentham in the 19th century, the Panopticon is an octagonal structure with rooms on each side, with windows opening towards the central watch-tower.
- This structure made disciplining possible, since it ensured the source of power was always present, though this could not be verified.
- When organisation implement rules of conduct and other monitoring policies, the Panopticon effect helps ensure conformity and discipline.
- IS have the Panopticon effect where employees are aware they are being monitored but are not sure.



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.





**THANK
YOU !**



NPTEL ONLINE CERTIFICATION COURSES

Management Information System

Saini Das

Vinod Gupta School of Management, IIT Kharagpur

Module 11: Ethical, social and security issues in MIS Security issues in MIS

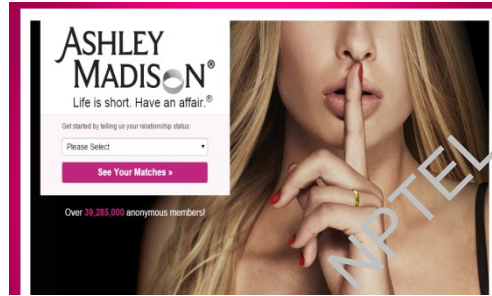
Apr 2019



May 2017



Jul 2015



Dec 2013

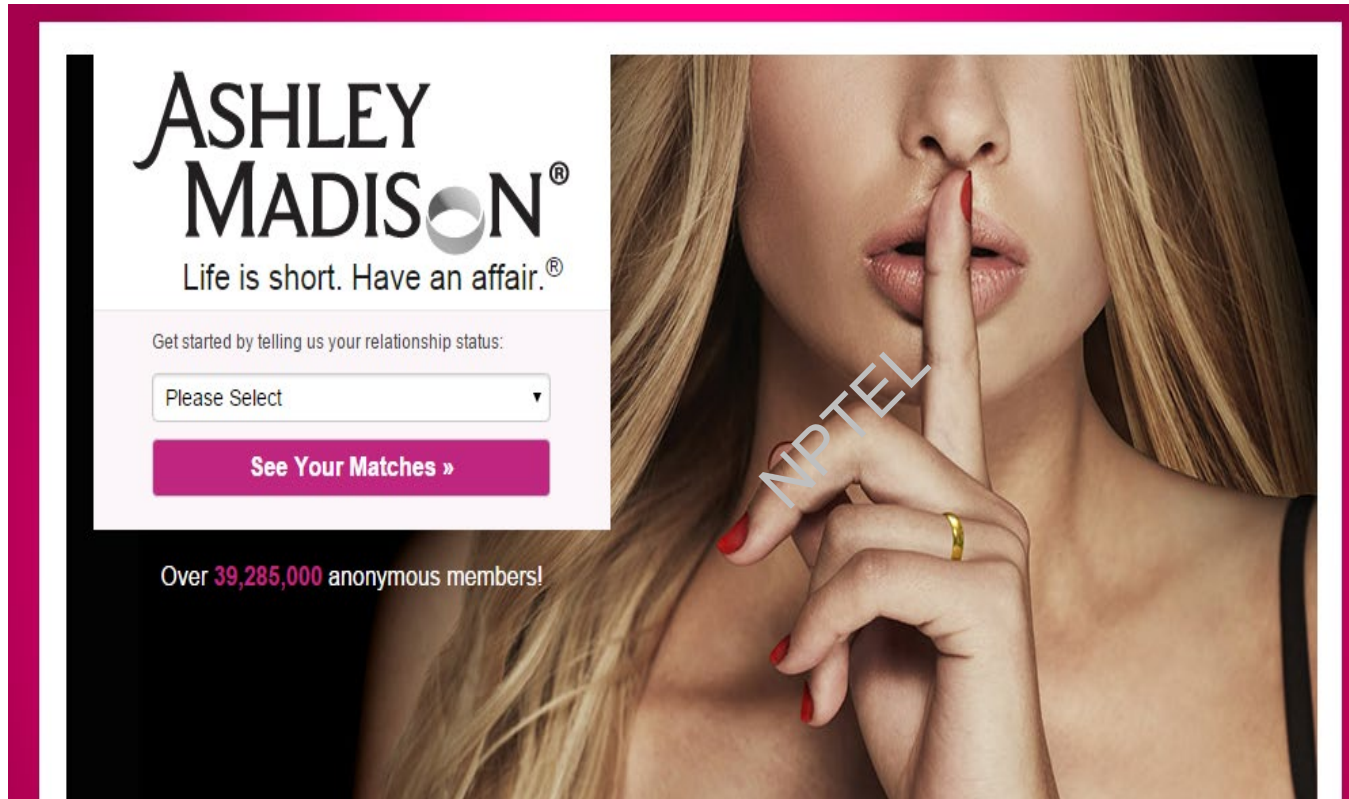


Apr 2011



?

Ashley Madison Data Breach



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

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.”

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

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

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

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?

Security Threats in Organizations

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.



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.



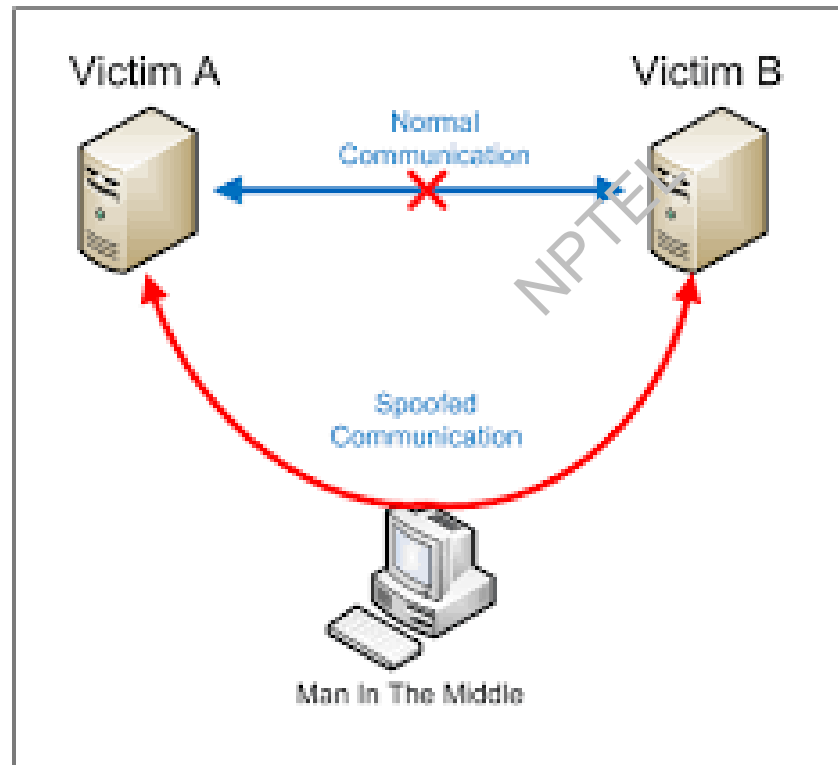
Website Defacement/Cyber Vandalism

- 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.



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.



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.



**THANK
YOU !**



NPTEL ONLINE CERTIFICATION COURSES

Management Information System

Saini Das

Vinod Gupta School of Management, IIT Kharagpur

Module 11: Ethical, Social and Security issues in MIS Security issues in MIS - II

Identity Theft

- Phishing attack
- Spear Phishing attack
- Pharming attack

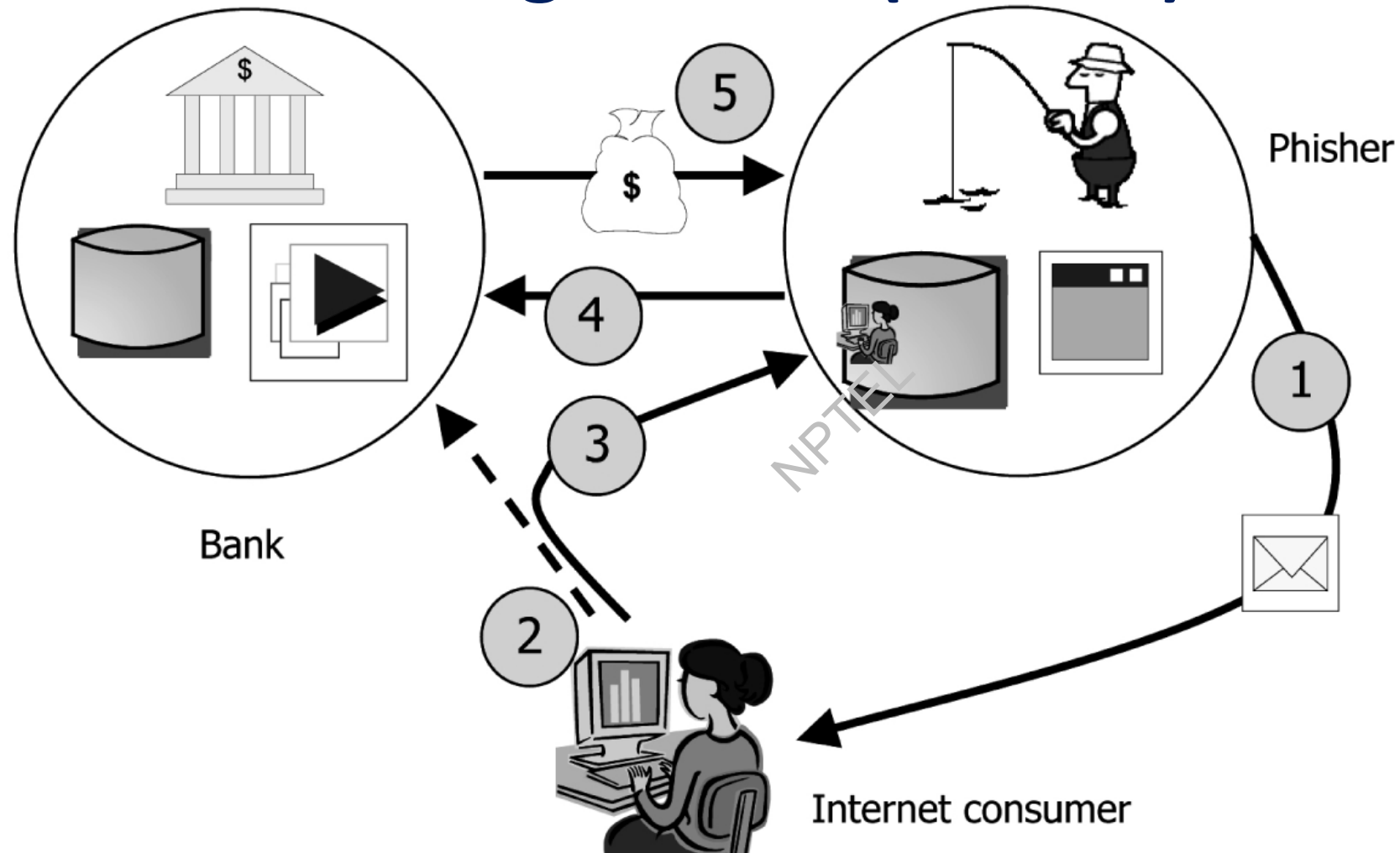
NPTEL

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



Phishing Attacks (contd..)





Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.


If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Spear Phishing Attacks

From: [redacted]
Date: 22 September 2010 16:06
To: [redacted]
Subject: Salaries 2011 (confidential) - Fixed
Attach:  new_salaries_2011.pdf (263 bytes)

Hi, here you have the fixed version of the salaries. Sorry about the errors in the yesterdays email...
Please let me know if you have any comments.

[redacted]

--

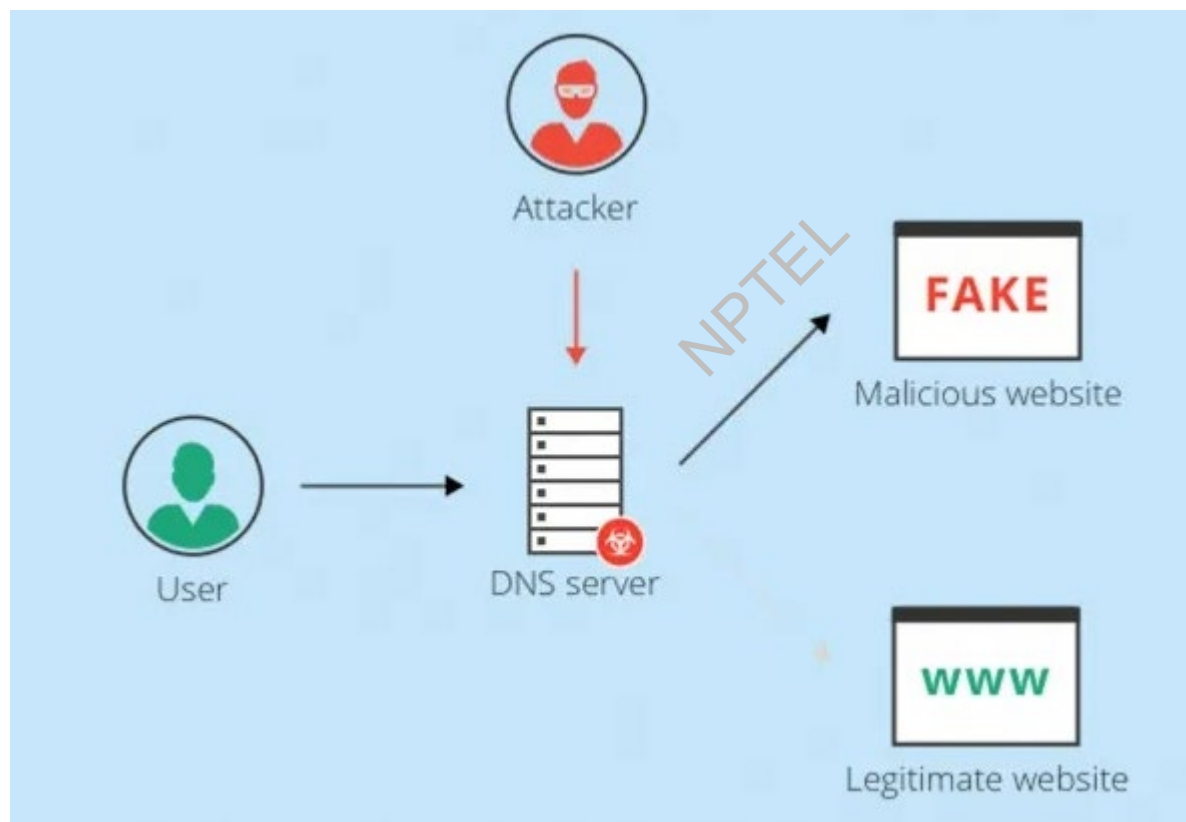
[redacted]
Human Resources and
Distribution Services
[redacted]



NPTEL

Pharming Attack

- Pharming redirects users to a bogus Web page even when the user types the correct website address into his or her browser.



Solutions

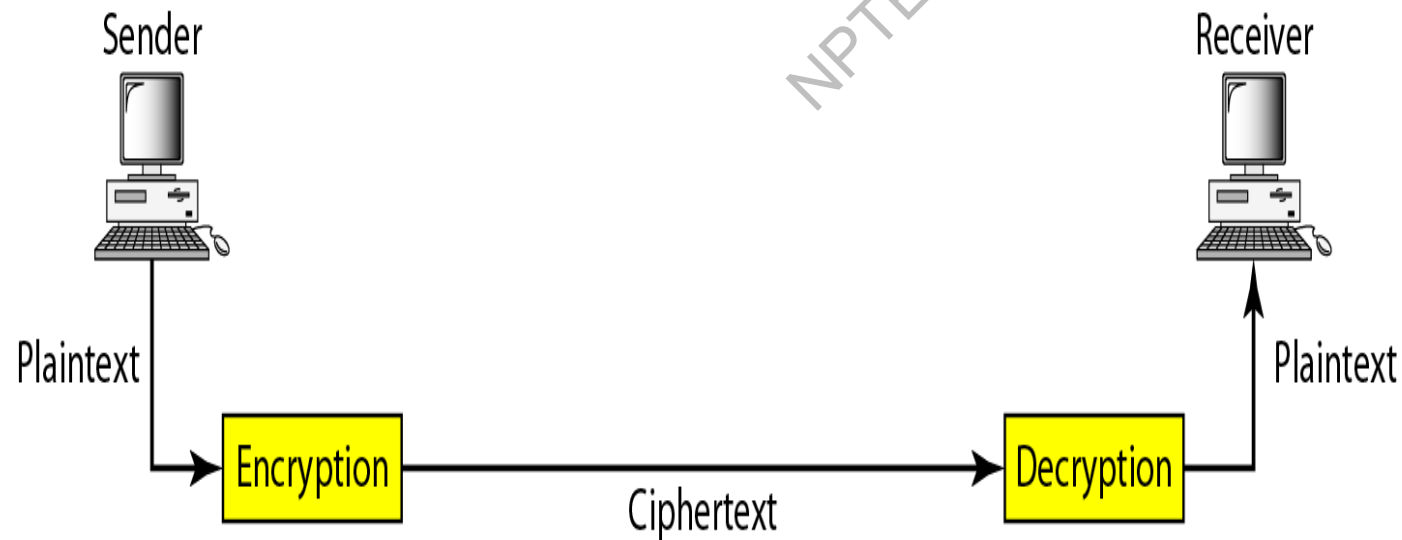
Organizational Security Environment



Technology Solutions

Encryption

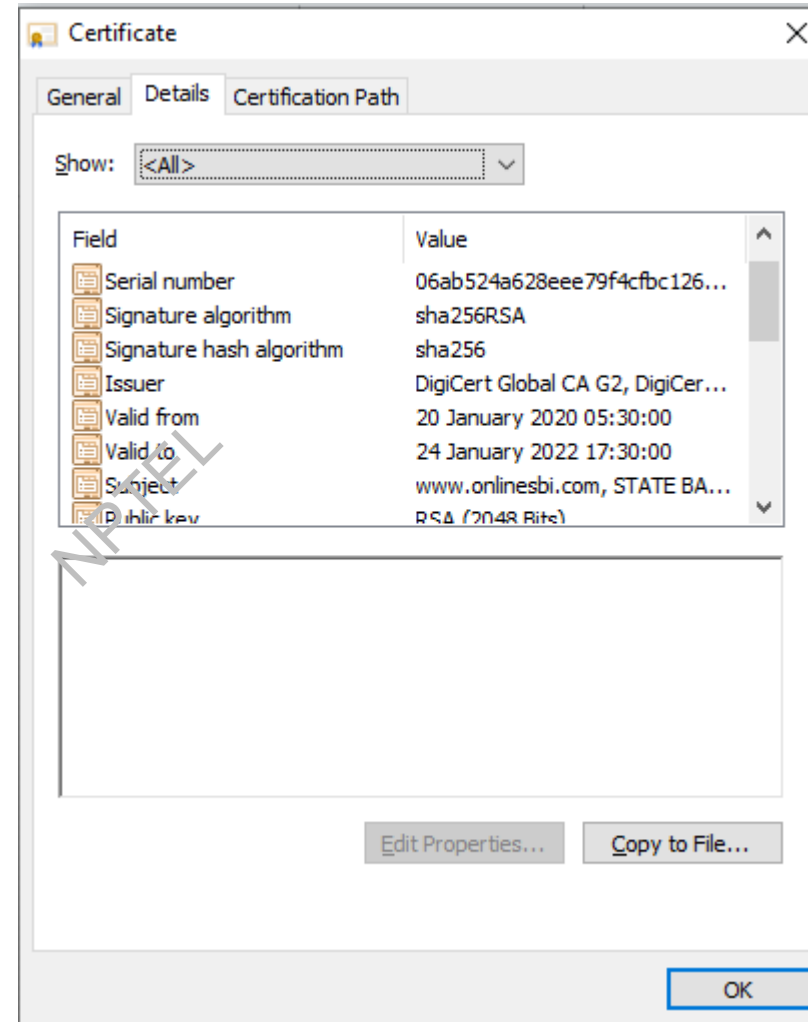
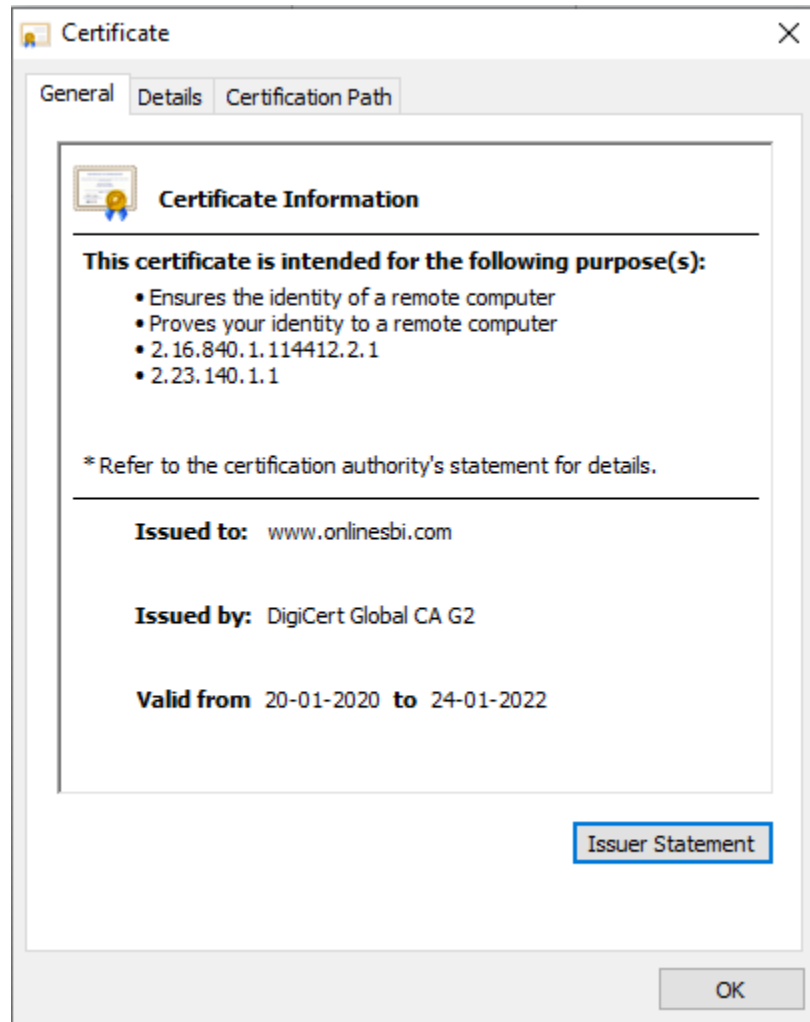
- Using a mathematics based program and a secret key to produce a string of characters that is unintelligible.
- Cryptography
 - Science and art that studies encryption



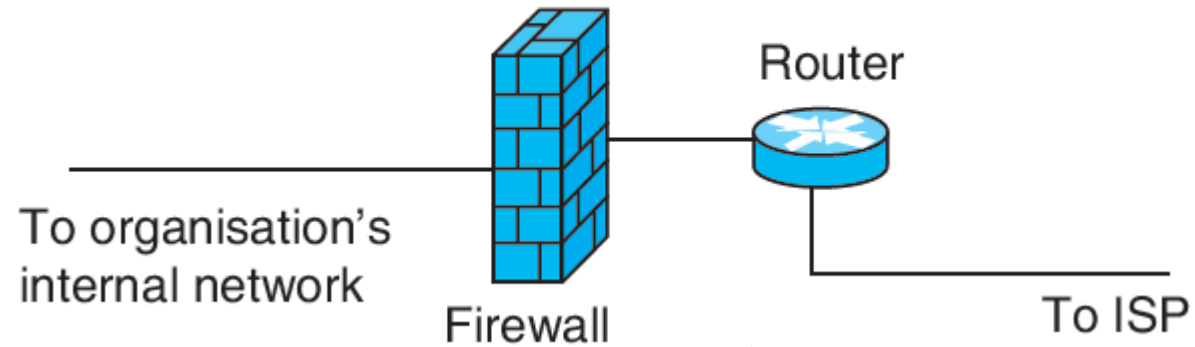
Digital Certificates

- 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

Digital Certificates (contd..)



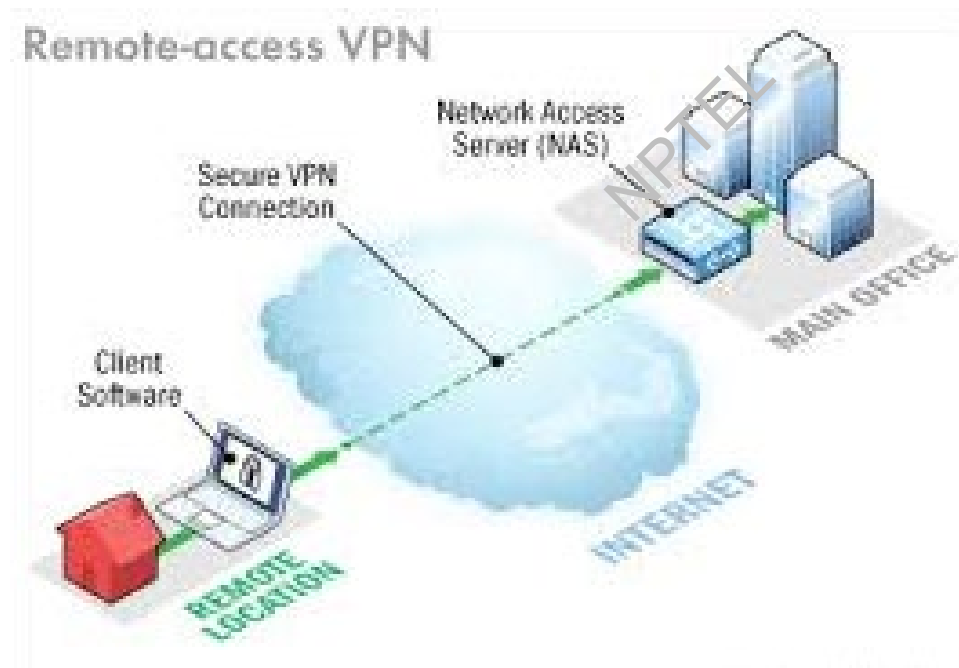
Firewall



- Firewalls are filtering and protection devices - usually a combination of hardware and software
- Packet-level filtering based on rules
- Firewalls slow down traffic at the perimeter – to overcome this firewalls are built into hardware.

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.



Phishing Attack Countermeasures

- Most important step that companies can take today is to educate web site users
- Many companies contract consulting firms that specialize in anti-phishing filters
- Report Phishing emails

www.millersmiles.co.uk

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.





**THANK
YOU !**



NPTEL ONLINE CERTIFICATION COURSES

Management Information System

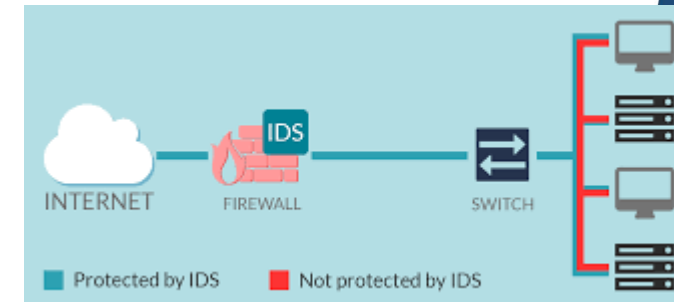
Saini Das

Vinod Gupta School of Management, IIT Kharagpur

Module 11: Ethical, Social and Security issues in MIS Security issues in MIS - III

Intrusion Detection Systems

- Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points or “hot spots” of corporate networks to detect and deter intruders continually.
- The system generates an alarm if it finds a suspicious or anomalous event.
- Scanning software looks for patterns indicative of known methods of computer attacks and sends warnings of vandalism or system administration errors.
- Monitoring software examines events as they are happening to discover security attacks in progress.
- The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.



Antivirus and Antispyware Software

- Antivirus software is designed to check computer systems and drives for the presence of computer viruses.
- Often the software eliminates the virus from the infected area.
- However, most antivirus software is effective only against viruses already known when the software was written.
- To remain effective, the antivirus software must be continually updated.
- Leading antivirus software vendors, such as McAfee, Symantec, and Trend Micro, have enhanced their products to include protection against spyware.



Unified Threat Management Systems

- A comprehensive appliance having various security tools, including firewalls, virtual private networks, intrusion detection systems, and anti-spam software.
- Helps businesses reduce costs and improve manageability.
- Although initially aimed at small and medium-sized businesses, UTM products are available for all sizes of networks
- Leading UTM vendors include Crossbeam, Fortinet, and Check Point.

Organizational Policies & Procedures

NPTEL

Organizational Security Plan



Risk Assessment

- Before a company commits resources to security it must know which assets require protection and the extent to which these assets are vulnerable.
- Risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled.
- IS specialists should try to determine the value of information assets, points of vulnerability, the likelihood of a problem, and the potential for damage.
- The expected annual loss for each exposure can be determined by multiplying the likelihood of a breach, and the potential for damage.
- Once the risks have been assessed, management will concentrate on the control points with the greatest vulnerability and potential for loss.

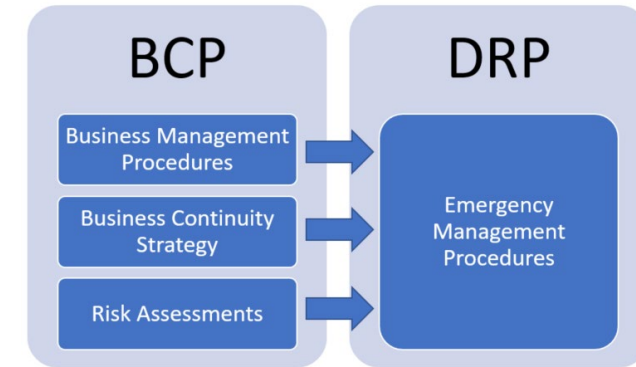
Security Policy

- Once the main risks to the systems have been identified, the company will need to develop a security policy for protecting the company's assets.
- A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving them.
- It drives policies determining acceptable use of the firm's information resources and which members of the company have access to those.



DRP/BCP

- Disaster recovery plan (DRP) devises strategies for the restoration of computing and communications services after they have been disrupted.
- DRP focuses primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.
- Business continuity plan (BCP) focuses on how the company can restore business operations after a disaster strikes.
- The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.



Security Audit

- Organizations must conduct comprehensive and systematic security audits.
- Security audits review technologies, procedures, documentation, training, and personnel.
- A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.



Legal and Regulatory Requirements

Cyber Laws

- Gramm-Leach-Bliley Act (1994): This act requires financial institutions to ensure the security and confidentiality of customer data.
- HIPAA (1996)
- Sarbanes-Oxley Act (2002): SOX is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Because information systems (IS) are used to generate, store, and transport such data, the legislation requires firms to consider IS security controls required to ensure the integrity, confidentiality, and availability of their data.

Computer Forensics

- Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law.
- It deals with the following problems:
 - Recovering data from computers while preserving evidential integrity
 - Securely storing and handling of recovered electronic data
 - Finding significant information in a large volume of electronic data
 - Presenting the information to a court of law



Organizations that Promote Computer Security

- **CERT**
 - Responds to thousands of security incidents each year
 - Helps Internet users and companies become more knowledgeable about security risks
 - Posts alerts to inform the Internet community about security events
- **Microsoft Security Research Group**
 - Privately sponsored site that offers free information about computer security issues

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.





NPTEL

THANK YOU !