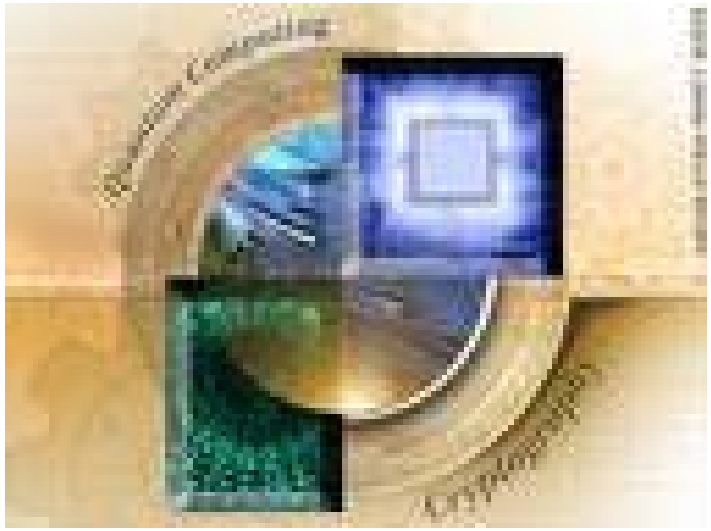
e-COMMERCE Perspectives

EDI
CYBER LAWS
CYBER SECURITY
IT ACT 2000

BY
JYOTINDRA ZAVERI
Cyber Security Consultant

PAPERLESS TRANSACTION

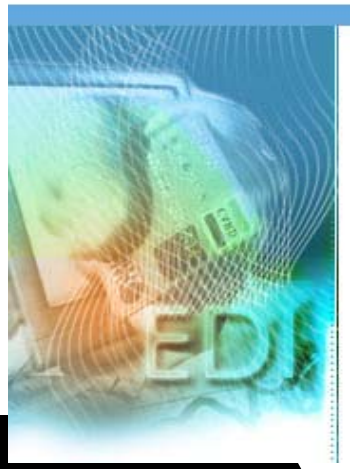
- HOW TO DO TRANSACTIONS ENTRIES INTO COMPUTER WITHOUT PAPER?
- FOR BUSINESS TO BUSINESS
  - E.G. SUPPLIER TO OEM (ORIGINAL EQUIPMENT MANUFACTURERS)
- ANSWER = EDI



WHAT IS EDI ?

- Electronic Data Interchange (EDI) is the transmission between businesses of information in standard, computer-readable format. It includes electronic order placement, electronic shipping notification, **electronic invoicing**, and many other business transactions that computers can actually perform better than people.
- EDI gives the necessary control to reduce unnecessary miscommunication
  - Which often disrupt the distribution process
- EDI **eliminates most of the data entry associated** with these functions
  - EDI eliminates the error that normally occurs in data entry environment.

ELECTRONIC DATA INTERCHANGE



E. D. I. INTERFACE

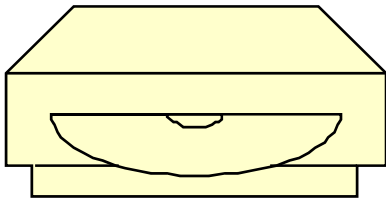
- TRADITIONALLY PAPER DOCUMENTS ARE GIVEN
  - E.G. INVOICE CUM CHALLAN PRINTED ON PAPER ALONG WITH MATERIAL
- Now, FLOPPY OR CD OR EMAIL IS GIVEN INSTEAD OF PAPER DOCUMENTS

E. D. I

ELECTRONIC DATA INSTEAD OF PAPER INVOICE GENERATED BY ERP SERVER AND READ ALSO BY ERP SERVER

PURCHASE ORDER BY EMAIL OR ON THE WEBSITE Or DATA RECORD

CUSTOMER



SUPPLIER OR VENDOR

MATERIAL SENT WITH EDI (CD)

WHAT IS DIGITAL SIGNATURE?

- AN ELECTRONIC, ENCRYPTION BASED, SECURE STAMP OF AUTHENTICATION ON DOCUMENT ORIGINATED FROM THE SIGNER (AND HAS NOT BEEN ALTERED)

WHAT IS DIGITAL CERTIFICATE ?

- DIGITAL CERTIFICATE IS ATTACHMENT FOR A FILE, OR EMAIL MESSAGE THAT VOUCHES FOR AUTHENTICITY, PROVIDES SECURE ENCRYPTION, OR SUPPLIES A VERIFIABLE SIGNATURE.

DIGITAL SIGNATURE

- PURPOSE
  - TO AUTHENTICATE TRANSACTION ON INTERNET
  - ATTACHED TO THE DOCUMENT – SIMILAR TO HANDWRITTEN SIGN
  - RECIPIENT CAN VERIFY THE DIGITAL SIGNATURE

E.G. 'REGISTRAR OF COMPANIES' (ROC) - RETURNS ARE FILED ONLINE USING DIGITAL SIGNATURE BY DIRECTORS, FOR LIMITED OR PRIVATE LIMITED COMPANIES

DIGITAL CERTIFICATES SIGNATURE FAQ

www.mtnltrustline.com/faq/faq1_2.htm

- DIGITAL SIGNATURES ARE USED THROUGH E-COMMERCE IN ORDER TO ENSURE THAT TRANSACTIONS ARRIVING AT A GATEWAY SERVER ARE FROM AN IDENTIFIABLE MERCHANT, AND THAT ANY INFORMATION PASSED BACK TO THE MERCHANT IS FROM A SECURE TRADING GATEWAY
- EACH SIGNATURE UNIQUELY IDENTIFIES ITS SOURCE.

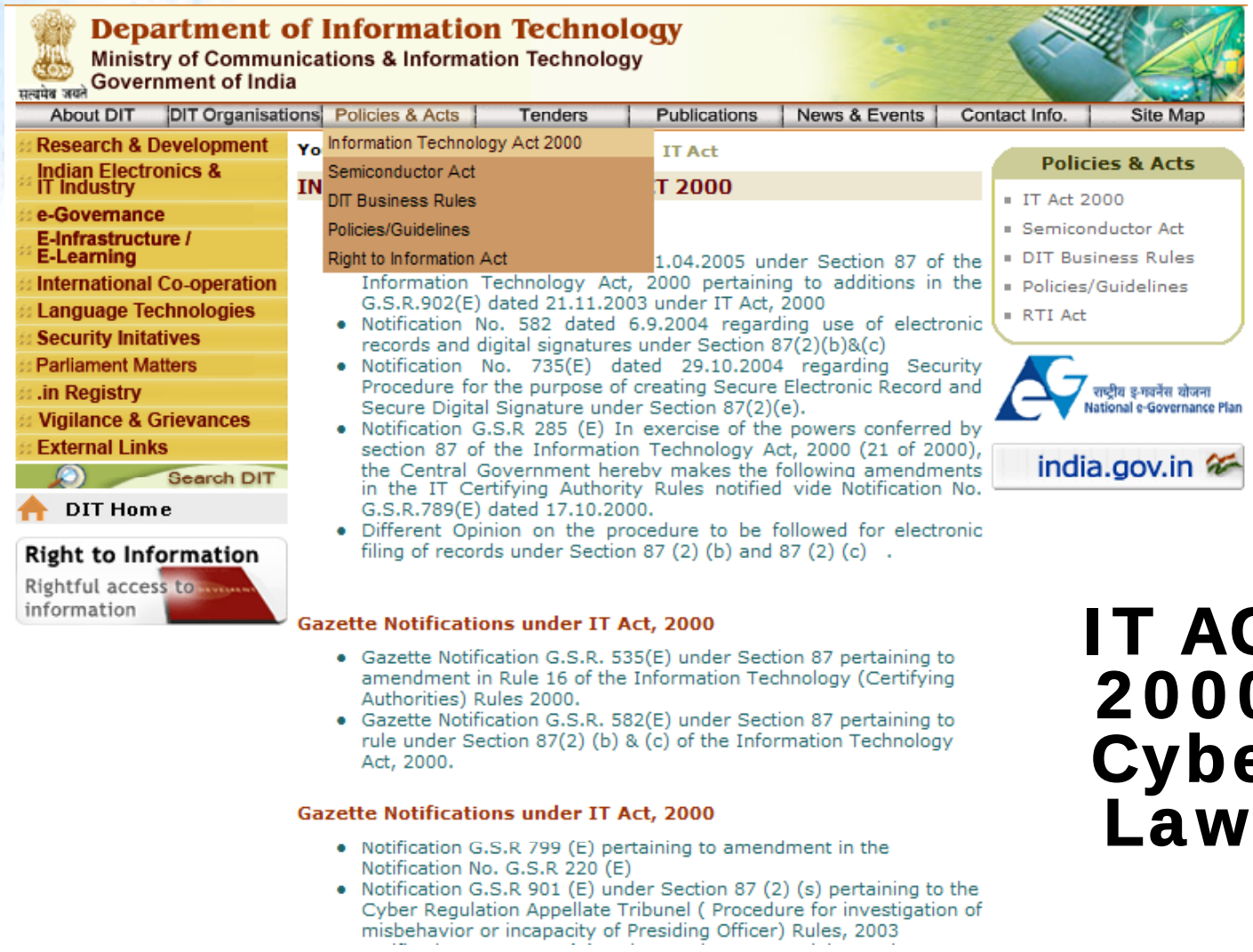
Cyber Laws

- What is the need for Cyber Laws?
- What is the need for Cyber Security?
  - What precautions to take to use e-Business and e-Commerce

Online Shopping

- Globally, e-Commerce is already > **$1.7 Trillion** industry and growing exponentially
- More and more people are doing online shopping
- Consumers are already buying online products and services
  - Bus or train or air tickets is common
  - Buying electronic gadgets, books, apparel, etc.

www.mit.gov.in



IT ACT 2000: Cyber Laws

Department of Information Technology
Ministry of Communications & Information Technology
Government of India

About DIT | DIT Organisations | Policies & Acts | Tenders | Publications | News & Events | Contact Info. | Site Map

- Research & Development
- Indian Electronics & IT Industry
- e-Governance
- E-Infrastructure / E-Learning
- International Co-operation
- Language Technologies
- Security Initatives
- Parliament Matters
- .in Registry
- Vigilance & Grievances
- External Links

Search DIT

DIT Home

Right to Information
Rightful access to information

You are here: Home > Policies & Acts > IT Act

INFORMATION TECHNOLOGY ACT 2000 Online

- PRELIMINARY
- DIGITAL SIGNATURE
- ELECTRONIC GOVERNANCE
- ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS
- SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES
- REGULATION OF CERTIFYING AUTHORITIES
- DIGITAL SIGNATURE CERTIFICATES
- DUTIES OF SUBSCRIBERS
- PENALTIES AND ADJUDICATION
- THE CYBER REGULATIONS APPELLATE TRIBUNAL
- OFFENCES
- NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES
- MISCELLANEOUS

Policies & Acts
- Government Policies
- IT Act
- R[illegible]Act
- Semiconductor Act
- CCA Office

National e-Governance Plan

india.gov.in

Disclaimer| Site Designed,Developed & Maintainted by C-DAC (A Scientific Society Under DIT)
This Site is best Viewed in 800X600 pixels.

Last Validated by: Ms. B. Vasanta, Scientist-F on December 26,2007

CYBER LAWS – IT ACT

I T ACT
IT BILL ONLINE

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as **"electronic commerce",** which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

ONLINE BANKING

- Accessing a bank account using internet is called ‘Online Banking’ or NET BANKING.
- E.g. **India’s largest bank: State Bank of India** has **11,100 branches**
- Number of people with access to internet banking has increased dramatically.
  - SBI has three million Net banking users
- **Websites are**
  - **www.sbi.co.in**
  - **www.onlinesbi.com**
  - **www.statebankofindia.com**

Unauthorized access to information on computer or website is called '**hacking**'

"SBI website falls victims to hacker. Attempts were made to disrupt the system from outside India".

- *Source: News in Economic Times & Business Line – 28 Dec 08.*

Mr. R. P. Sinha,
Deputy M. D. SBI.

IT ACT 2000:
Under Section 66
Hackers can be
punished.

IT ACT 2000: Cyber Laws

Data Alteration

- Section 66 of the IT Act covers unauthorized alteration of data. This section deals with **hacking**. According to this section, unauthorized alteration of data is punishable.

Unauthorized Access

- Section 43 covers the crimes related to the unauthorized access.

IT ACT 2000: Cyber Laws

- **Virus & malicious code**
- Introduction of a computer virus or contaminant (including worms, Trojans, etc.) is covered by Section 43 of IT Act.
- Section 65
  - Crimes relating to source code.
  - Software piracy is illegal.
- Posting remarks on website against the Government of India or Indian constitution is illegal
- Creating an email account on false name is illegal

Can such crimes be detected?

- YES
  - Each time you log on to the internet, you are allotted an IP address, which is very easy to trace within a matter of minutes and in some cases hours

How do you catch cyber criminals?

- Every e-mail leaves behind a trace leading back to its point of origin in the form of an e-mail header. To view the header all you need to do is to press 'options' button and then go to 'preferences‘
- This will throw up two boxes where you can view your e-mail in full, complete with the IP addresses. The IP address, usually a number like 61.1.92.199, can be traced to ISP (VSNL).
- But only the police have the authority to trace back the route of the message beyond this point right up to the doorstep of the offending subscriber.

Unique IP address of origin of email

Return-Path: <mjcjal_jal@sancharnet.in>
Delivered-To: zaveri.pn1@pn123.vsnl.net.in
Received: from mx2.vsnl.com (mx2.vsnl.com [202.54.1.74])
by pn123.vsnl.net.in (Postfix) with ESMTP id 8ED75B472
for <zaveri@giaspn01.vsnl.net.in>; Mon, 16 Dec 2002 17:39:25 +0530 (IST)
Received: from ndl1mr1-a-fixed (avmx2.vsnl.com [202.54.1.76])
by mx2.vsnl.com (Postfix) with ESMTP id 638C565B2
for <jyotindra@vsnl.com>; Mon, 16 Dec 2002 17:39:41 +0530 (IST)
Originating-IP: 61.1.92.199
(iPlanet Messaging Server 5.2 HotFix 0.9 (built Jul 29 2002))
with ESMTP id <0H7700EJKOCW9X@ndl1mr1-a-fixed.sancharnet.in> for
jyotindra@vsnl.com; Mon, 16 Dec 2002 17:37:44 +0530 (IST)
Date: Mon, 16 Dec 2002 17:37:44 +0530 (GMT+05:30)
From: mjcjal_jal@sancharnet.in
Subject: Invitation
X-Originating-IP: 61.1.92.199
To: jyotindra@vsnl.com

Email spoofing

- E-mail spoofing is a problem
  - Fake email, where an email appears to be sent by someone but has actually been sent by some other person, has brought many to financial ruin.
- Email spoofing is covered under provisions of the IPC relating to forgery.

Email messages can be fake

- E.g. An Indian bank which recently faced a serious problem, because email, supposedly sent by its manager, informed customers that the bank was facing financial troubles (rumor)
- A businessman was conned out of Rs 10 lakhs by a Nigerian who was pretending to be the Vice President of the African Development Bank
  - The businessman trusted the senders email address as was showing in the email that he received.
- **The only way to protect yourself is to <u>digitally sign</u> and encrypt all important email messages**

Educate people

- 99% of people by and large think that e-mail address cannot be traced but if they come to know that almost all the cases, no matter what wrong name they give, what e-mail address they open, they can still be traced then the cyber crime rate will fall
- It is just a matter of education
  - Newspapers and magazines have major role to play in curbing, educating public on cyber crimes.

DIGITAL EVIDENCE

What is Digital Evidence?

- Digital evidence is any information of probative value that is either stored or transmitted in a binary form. This field includes not only computers in the traditional sense but also includes digital audio and video. It includes all facets of crime where evidence may be found in a digital or binary form. Computers are also instrumental in crimes ranging from check fraud to conspiracy.

Cyber Crimes

- Learn from security and forensics networks
  - The good part is, lots of information is available on training programs and conferences about computer forensics. E.g.
    - Def Con (http://www.defcon.org/) stages conventions about hacking
    - Black Hat (www.blackhat.com) offers conventions, security conferences, and training – Digital self defense

Phishing Sites

- *Phising* pronounced ‘fishing’ refers to fishing out sensitive user information such as your credit card number
- This is done by masquerading (Camouflaged) as a trustworthy entity. This usually is an email with clickable hyper link. This email comes to your inbox with a familiar bank name as a **disguise**.
- Say, you have account in ICICI bank. The email will come as if from ICICI and ask you to click on a link. This will take you to a similar website (as if it is ICICI bank) and ask you to enter credit card number.

What is the difference between http and https?

- General websites use the standard **protocol** known as Hyper Text Transfer Protocol.
  - This sites may not be secured.
  - Think twice before parting with credit card information.
    - Chances of hacking is very high
    - Not secured websites.
- https:// is a protocol which is secured.
  - Websites using https protocol incorporates some kind of encryption technology such as SSL (Secured Socket Layer), provided by companies like **verisign.com**.
    - It is safe to give credit card kind or sensitive information to such websites because it is secured.
    - Hackers will not be able to get user's confidential data.
- E.g. Look for http**s**://www.xyzbank.com – that **s** after http is important.
- Most e-commerce website with payment gateway uses **https** protocol.

Minimize RISK
Security tips: Do and Do Not

Configure your PC security OS settings, to automatically update the virus protection and keep it up-to-date

- E.g. AVG website or Quick Heal, etc.

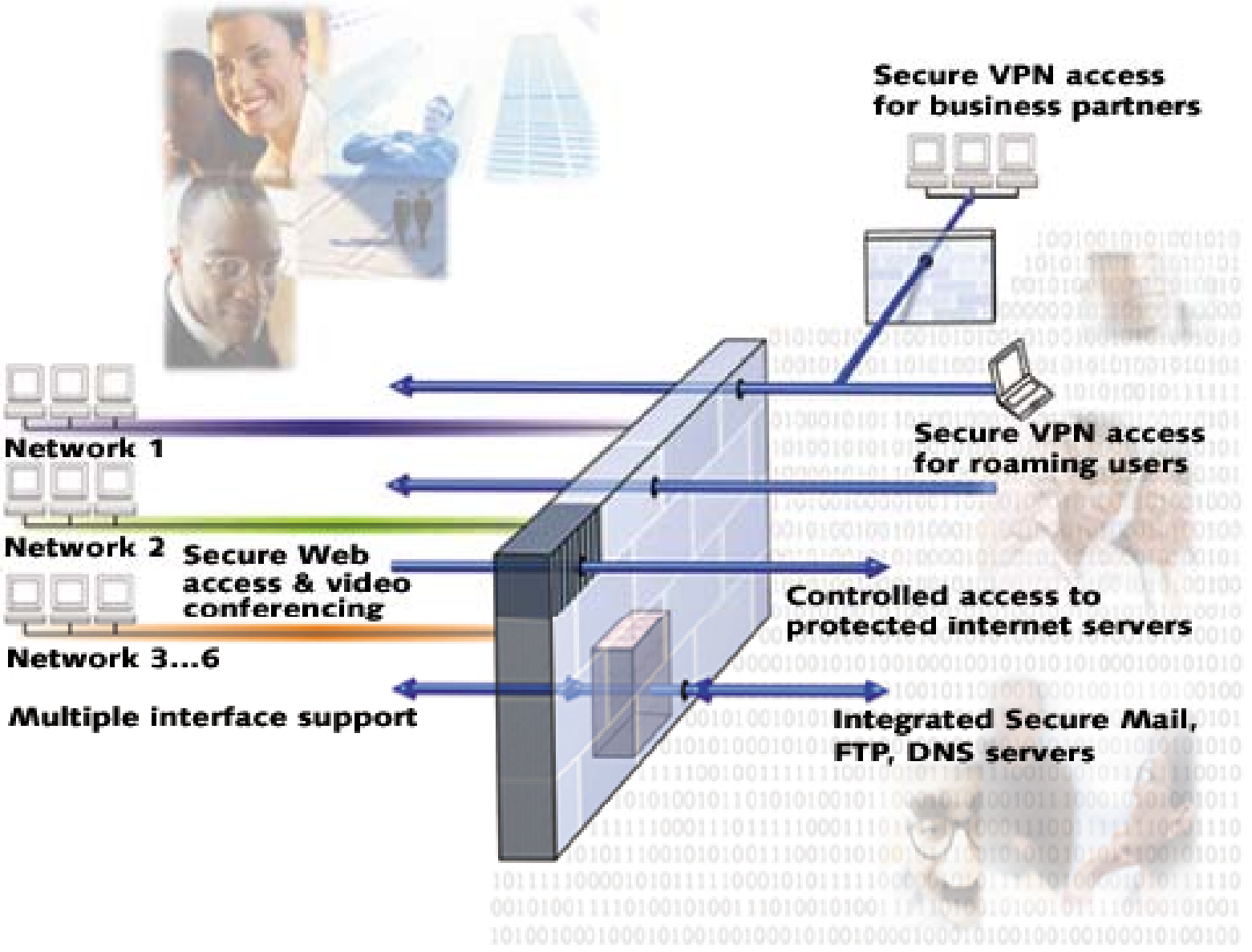
Configure proper security settings for your Browser (Internet Explorer) based on your surfing requirements. E.g. Cooky setting

Avoid free software downloads such as free wall papers, free screen savers, etc. It may contain virus – along with it some unwanted software may also get installed

Safety norms for doing on-line banking

- Make sure that the banking website address starts with https (SSL protected) which ensures encryption protected communications.
- Never do online banking transactions on a shared or public computer – e.g. Cybercafé.
- Always type the web address of your bank into the browser space. Never click on the link in the email.
- Deploy anti-spy ware, **Firewall**, Anti-Phishing, Anti-Spam, Piracy protection software.

Fire – wall: Protection software



Firewall

- The Firewall Software consists of programs designed to monitor and control the flow of traffic between computers and networks.
- Firewalls are generally used to prevent unauthorized access to computers or networks.
- Firewall can allow, restrict, encrypt, based on settings and definitions such as trust levels.

Authentication

- In a multi-user or network environment, the process by which the system validates a user's logon information. A user's name and password are compared against an authorized list, and, if the system detects a match, access is granted to the extent specified in the permission list for that user.
- **Authentication database**
  - A database on a server that matches user names to passwords.

Threat Categories ☹

- Natural Disasters – Fire, flood, tornado, etc.
- Nonhuman – Product failures, bugs, etc.

Human

- Malicious code
- Insiders – Disgruntled employees
- Outsiders – Hackers
- Non-malicious: Untrained or uninformed employees (careless)
  - E.g. password is not kept secret

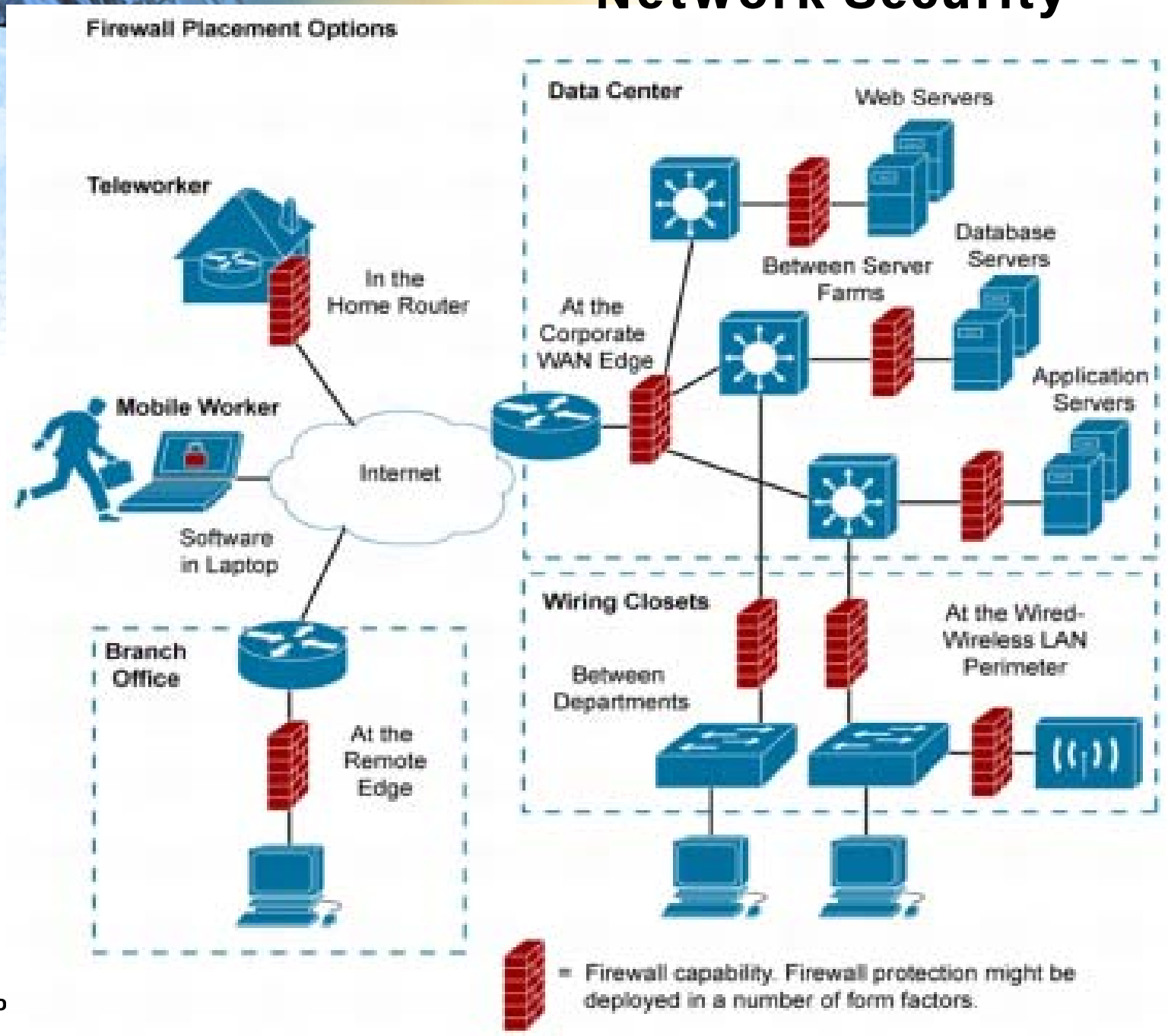
What is security?

- ***Security means:*** Measures taken to guard against espionage or sabotage, crime, attack, or escape.
- Precautions:
  - Do not give credit card / debit card information to unbranded website or unknown person.
  - Use Debit card instead of Credit card.
  - Never put too much of personal information on the social website like ‘Orkut’.

What is Cryptography ?

- Cryptography is the science of writing in secret code.
- Cryptographic protocols can provide us new application paradigms, which were not achieved without cryptography. For examples, using cryptographic protocols, we are able to establish electronic payment systems, electronic elections systems, electronic auction system, etc. Some of them have been used in practical fields. They are becoming the fundamental infrastructure of electronic society.

Network Security



Compute safely

THANK YOU

Jyotindra Zaveri

Cyber Security Consultant

j.zaveri@dnserp.com

www.dnserp.com