Cyber Law

educlash.com
Just another Way To Learn

CYBER LAW ?

- Cyber Law is the law governing cyber space.It protects the activities on internet and other online communication technologies
- Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace.
- As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyberlegal perspective.

Importance of Cyber Law

- We are living in highly digitalized world.
- All companies depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.

Importance of Cyber Law

- Most people are using email, cell phones and SMS messages for communication.

- Even in "non-cyber crime" cases, important evidence is found in computers /cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.

- Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber Law is extremely important.

Need of Cyber Law

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

National Research Council, 1991.

Need of Cyber Law

- Internet has dramatically changed the way we think, the way we govern, the way we do commerce and the way we perceive ourselves.
- Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies.
- The laws of real world cannot be interpreted in the light of emerging cyberspace to include all aspects relating to different activities in cyberspace

Cyber Jurisprudence

- Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law.

- Jurisprudence refers to two different thing:
  1. Philosophy of law or Legal Theory
  2. Case Law

- Cyber jurisprudence deals with the composite idea of cyber jurisdiction and cyber court's venue in the cyberspace. It emphasis to recognize cyber uniform rules and policies at international level,

Cyber law in india

IT Act-2000

- **The Information Technology Act, 2000 (IT Act), came into force on *17 October 2000.***

- **The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.**

- **Information Technology Act 2000 consisted of *94 sections* segregated into *13 chapters*.**

Scope of Cyber Law

- Cyber Crimes
- Data Protection and Privacy
- Intellectual Property
- Electronic or Digital Signatures

Cyber Crime ?

- Any crime with the help of computer and a networking technology.

- Any crime where either the computer is used as an object or subject.

- Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both.

Various categories of Cyber-Crime:

Cyber Crime may be basically divided into 3 categories-

- Against Persons
- Against Property
- Against Government

Against Person:

- **Cybercrimes committed against persons include various crimes like:**

  - **Cyber stalking**
  - **Defamation**
  - **Spamming,spoofing.**
  - **Transmission of Obscene Material/Cyber pornography.**

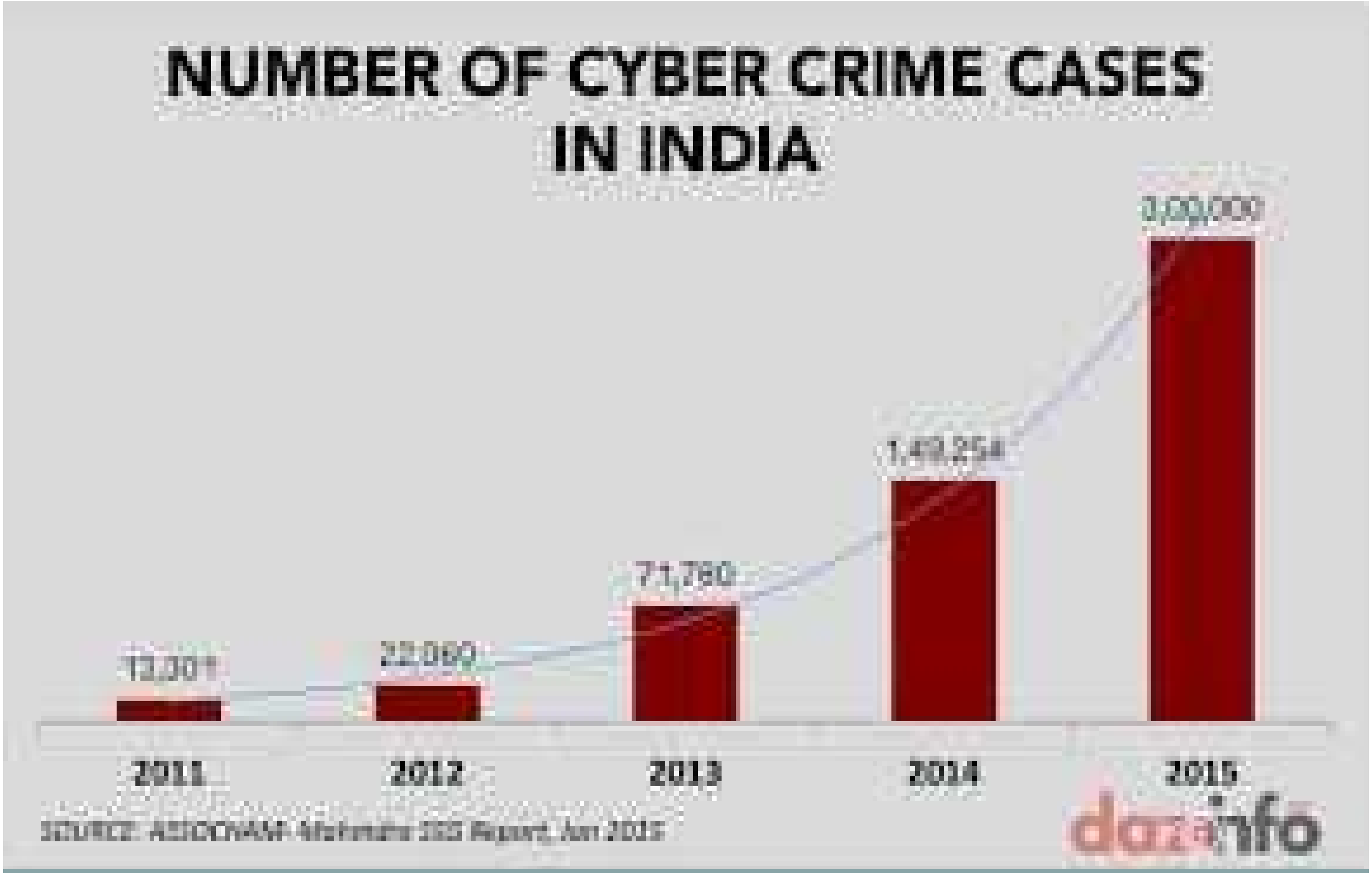
Against Property:

- The second category of Cybercrimes is that of Cybercrimes against all forms of property. These crimes include:
  - ➢ Unauthorized Computer Trespassing
  - ➢ Computer vandalism
  - ➢ Cyber squatting
  - ➢ Hacking Computer system

Against Government:

- The third category of Cybercrimes relate to Cybercrimes against Government.
- It includes:
  - Hacking of Government websites
  - Cyber Extortion
  - Cyber Terrorism
  - Computer Viruses

Statistics of Cyber Crimes



SOURCE: ASSOCHAM- Mahindra SSG Report, Jun 2015

TYPES OF CYBER CRIME

- **Hacking**
- **Cyber pornography**
- **Spamming**
- **Spying**
- **Online frauds**
  - Phishing
  - Cyber vandalism
  - DOS attack
  - Trojan
  - Viruses
- **Cyber Terrorism**
- **Illegal Trading**
- **Cyber Harrassment**

Types of cyber crime

- **HACKING** :- Hacking in simple terms means an illegal intrusion into a computer system and/or network . It is also known as CRACKING. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage.

Motive behind the crime called hacking greed power, publicity, revenge, adventure desire to access forbidden information destructive mindset.

- **Cyber Pornography**:Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

TIME
CYBERPORN
EXCLUSIVE: A new study shows how pervasive and wild it really is.
Can we protect our kids—and free speech?

- As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of Pedophiles.

  How Do They Operate :

  How do they operate Pedophiles use false identity to trap the children , Pedophiles connect children in various chat rooms which are used by children to interact with other children.

- **SPAMMING: Spamming** is the use of electronic messaging systems to send unsolicited messages (**spam**) for commercial or fraud purpose. While the most widely recognized form of spam is e-mail spam

- **SPYING:**Cyber spying is a form of cybercrime in which hackers target computer networks in order to gain access to classified or other information that may be profitable or advantageous for the hacker. Cyber spying is an ongoing process that occurs over time in order to gain confidential information. It can result in everything from economic disaster to terrorism.

The potentially harmful outcomes of cyber spying not only cause government security breaches but can also lead to the declassification of company secrets. This can be disastrous for companies if the attackers use stolen information to manufacture copy-cat products and gain market share.

- **ONLINE FRAUDS**

❑ **PHISHING:** “ Phishing” or “Web spoofing” attacks use fraudulent Web sites to trick you into giving away confidential personal information such as credit card numbers, account usernames and passwords, and ID numbers. This is called “phishing” because attackers are “fishing” for your personal information and trying to lure you into providing it.

❑ **CYBER THEFT:**Stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use.

- **ONLINE FRAUDS**

  - **DENIAL OF SERVICE ATTACKS :** This is an act by the criminals who floods the bandwidth of the victims network or fills his E-mail box with spam mail depriving him of the service he is entitled to access or provide. Many DOS attacks, such as the ping of death and Tear drop attacks.
  - **VIRUS DISSEMINATION :** Malicious software that attaches itself to other software. VIRUS , WORMS, TROJAN HORSE ,WEB JACKING, E-MAIL BOMBING etc.
  - **COMPUTER VANDALISM :** Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. These are program that attach themselves to a file and then circulate.

- **CYBER TERRORISM:** Cyber terrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.
- **HARRASSMENT:** Harassment includes directing obscenities toward others, as well as making derogatory comments based for example on gender, race, religion, nationality, sexual orientation. Unsolicited email messages and advertisements can also be considered to be forms of Internet harassment where the content is offensive or of an explicit sexual nature.
- **ILLEGAL TRADING:** Sale of illegal article.This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

DIGITAL SIGNATURE

Why Digital Signatures?

- To provide Authenticity, Integrity and Non -repudiation to electronic documents

- To use the Internet as the safe and secure medium for e-Governance and e-Commerce

DIGITAL SIGNATURE

What is Digital Signatures?

- A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender can not easily repudiate it later.
- Concept is based on method of cryptography.
- The originator of a message uses a signing key (Private Key) to sign the message and send the message and its digital signature to a recipient
- The recipient uses a verification key (Public Key) to verify the origin of the message and that it has not been tampered with while in transit

CRYPTOGRAPHY

- Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

DIGITAL SIGNATURE

Digital signatures employ a type of Asymmetric Cryptography. The Scheme typically consists of three Algorithms

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity

Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document

DIGITAL SIGNATURE

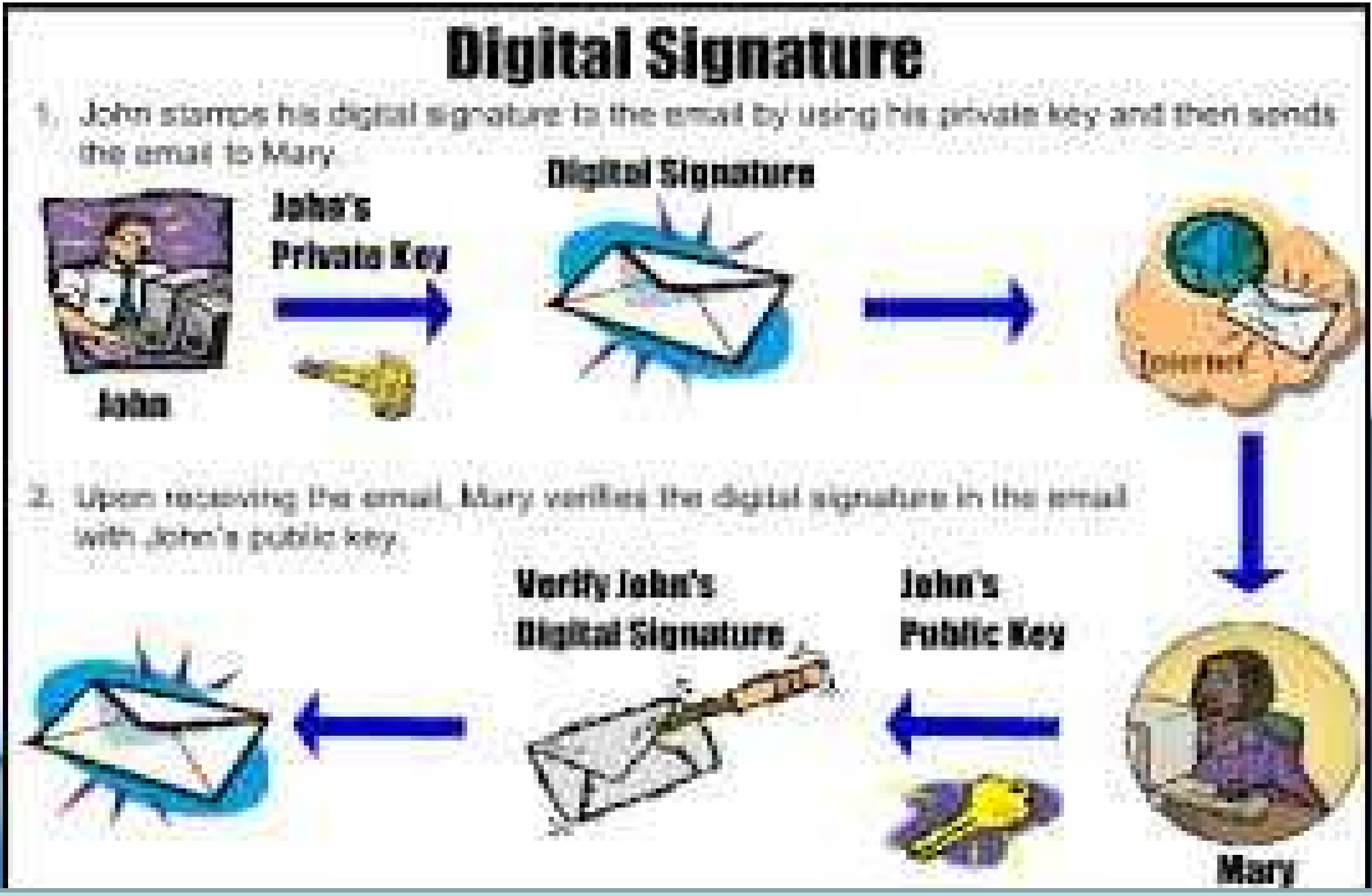
Each individual generates his own key pair

[Public key known to everyone
&
Private key only to the owner]

Private Key – Used for <u>making</u> Digital Signature

Public Key – Used to <u>verify</u> the Digital Signature

DIGITAL SIGNATURE



Digital Signature

1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.

2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.

DIGITAL SIGNATURE

Certifying Authorities

Certificate Authority (CA) is a trusted entity that issues Digital Certificates and public-private key pairs. The role of the Certificate Authority (CA) is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

Certificate Authority (CA) is a critical security service in a network.

DIGITAL SIGNATURE

A Certificate Authority (CA) performs the following functions.

Certificate Authority (CA) Verifies the identity: The Certificate Authority (CA) must validate the identity of the entity who requested a digital certificate before issuing it.

Certificate Authority (CA) issues digital certificates: Once the validation process is over, the Certificate Authority (CA) issues the digital certificate to the entity who requested it. Digital certificates can be used for encryption (Example: Encrypting web traffic), code signing, authentication etc.

Certificate Authority (CA) maintains Certificate Revocation List (CRL): The Certificate Authority (CA) maintains Certificate Revocation List (CRL). A certificate revocation list (CRL) is a list of digital certificates which are no longer valid and have been revoked and therefore should not be relied by anyone.

DATA PROTECTION AND PRIVACY

Privacy on the Internet depends on your ability to control both the amount of personal information that you provide and who has access to that information

INTRODUCTION

Maintaining your privacy requires you to take a multi-pronged approach. It involves protecting your sensitive information by preventing, detecting, and responding to a wide variety of attacks. There are many potential risks to your computer. Some are more serious than others. Among these dangers are:

- Viruses corrupting your entire system
- Someone breaking into your system and altering files
- A hacker using your computer to attack others
- Someone stealing your computer and accessing your personal information

There's no guarantee that even with the best precautions some of these things won't happen. However, you can take steps to minimize the risks to your computer and your sensitive information. Ultimately, the security of your computer is dependent upon you.

Ensuring privacy

Privacy software is software built to protect the privacy of its users. The software typically works in conjunction with Internet usage to control or limit the amount of information made available to third parties. The software can applyencryption or filtering of various kinds.

Ensuring privacy

- Privacy software can refer to two different types of protection. One type is protecting a user's Internet privacy from theWorld Wide Web. There are software products that will mask or hide a user's IP address from the outside world in order to protect the user from identity theft.
- The second type of protection is hiding or deleting the users Internet traces that are left on their PC after they have been surfing the Internet. There is software that will erase all the users Internet traces and there is software that will hide and encrypt a user's traces so that others using their PC will not know where they have been surfing.

Intellectual property

- Intellectual property (IP) theft is defined as theft of material that is **copyrighted**, the theft of **trade secrets**, and **trademark** violations.

- Theft of copyrighted material involves Stealing,Copying ,Distributing computer software, recorded music, movies, and electronic games.

Intellectual property

- Theft of trade secrets means the theft of ideas, plans, methods, technologies, or any sensitive information from all types of industries including manufacturers, financial service institutions, and the computer industry.Theft of trade secrets damages the competitive edge and therefore the economic base of a business.
- A trademark is the registered name or identifying symbol of a product that can be used only by the product's owner. A trademark violation involves counterfeiting or copying brand name products such as well-known types of shoes, clothing, and electronics equipment and selling them as the genuine or original product.

Intellectual property

- IP pirates never have to make sales in person or travel, their costs are minimal, and profits are huge.
- Internet pirates target the online shoppers who look for discounted, but legitimate, products.
- They do so by emails and Internet advertisements that seem to be the real thing.
- Not just individuals, but companies, educational institutions, and even government agencies have been tricked by IP pirates into buying stolen goods.

THANK YOU

educlash.com
Just another Way To Learn