ITEC614 Introduction to Cyber Security

Information Technology, PFBS

Fundamental Issues in Cyber Security

Lecture 1

Outline

- What is security?

- Security goals

- Cyberspace, Cybercrime, Cybersecurity

- Security risks

- Identity theft

- Countermeasures

Reference

This lecture is based on

Online resources. Most of the contents of this lecture is excerpted from the following site.

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

Security & Security Goals

What is Security?

Security according to 10 years old boys/girls

What is Security?

Security according to junior high school ICT teacher

What is Security?

Definition of Security

There is no straight forward definition!

Security is a process, not an end state!

Security is a process of maintaining an acceptable level of perceived risk.

Definition of Security

No organization can be considered "secure" for any time beyond the last verification of adherence to its security policy.

If your manager asks, "Are we secure?"
you should answer, "Let me check."
If he or she asks, "Will we be secure tomorrow?
" you should answer, "I don't know."

Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

Security Goals

Assurance that information is shared only among authorized persons or organizations.
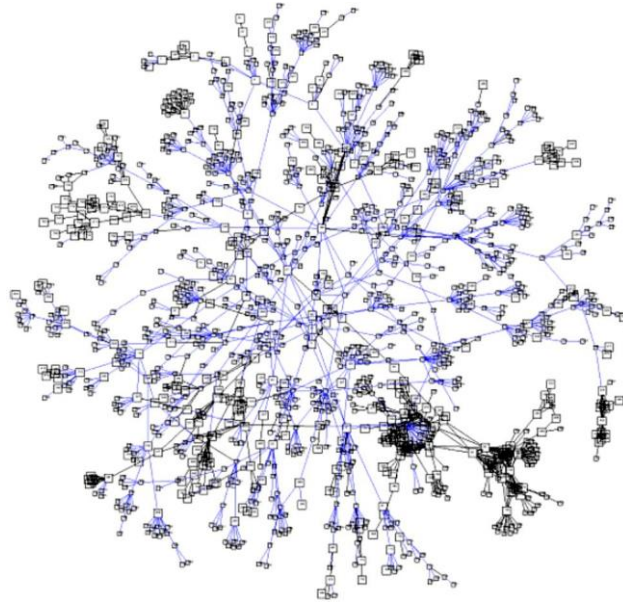

Assurance that the information is authentic and complete.

Availability of information refers to ensuring that authorized parties are able to access the information when needed

Concept of Cyberspace

Concept of Cyberspace

Cyberspace is "the environment in which communication over computer networks occurs."

Almost everybody in one way or the other is connected to it.

Cyberspace

Ladies in the market are connected to is to run their businesses

Shepherds are connected to locate their cattle

Hunters are connected to it to locate their prey

Cyberspace

Hmmm! isn't amazing?
They are also connected.

Cyberspace

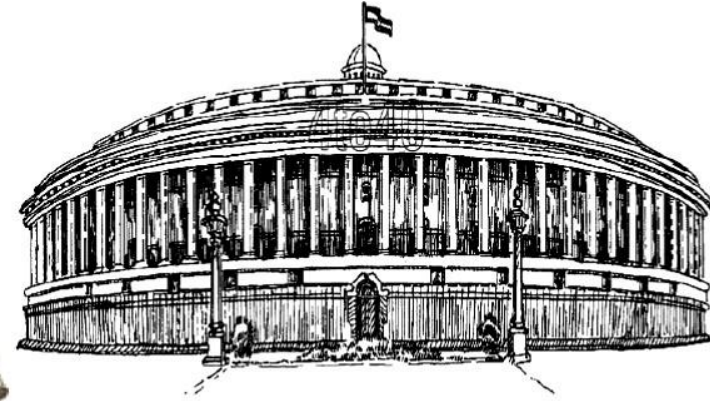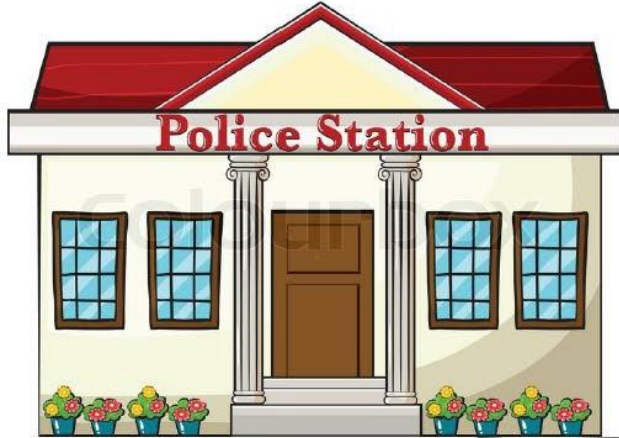On a more serious note, are connected

Government

Judiciary

Law makers

Cyberspace

Militaries

Cyberspace

Banks

Transportation Sectors

Health Sectors

Cybercrime & Cyberwar

Cybercrime

Computer crime, or cybercrime, is any crime that involves a computer and a network.

The computer may have been used in the commission of a crime, or it may be the target.
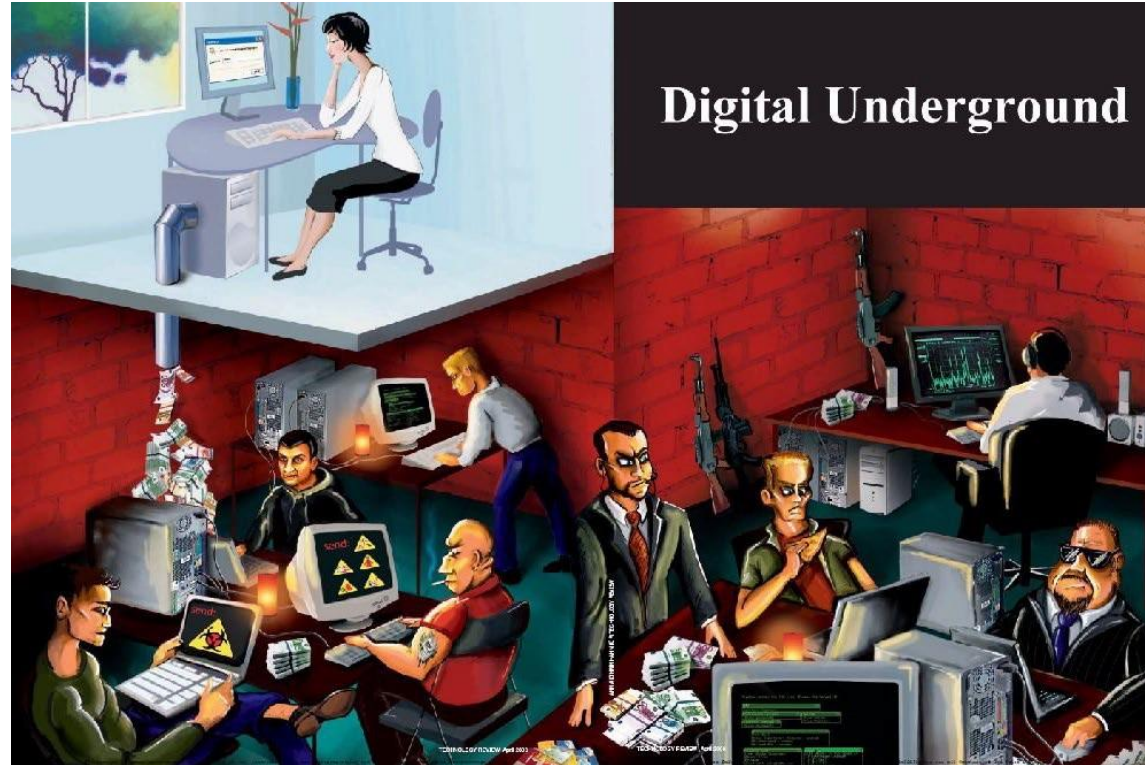
Cybercrime

Commonwealth Bank, Australia -March 2011:-Automatic teller machines (ATMs) spat out tens of thousands of free dollars in Sydney after a computer glitch turned into a nightmare for the Commonwealth Bank.
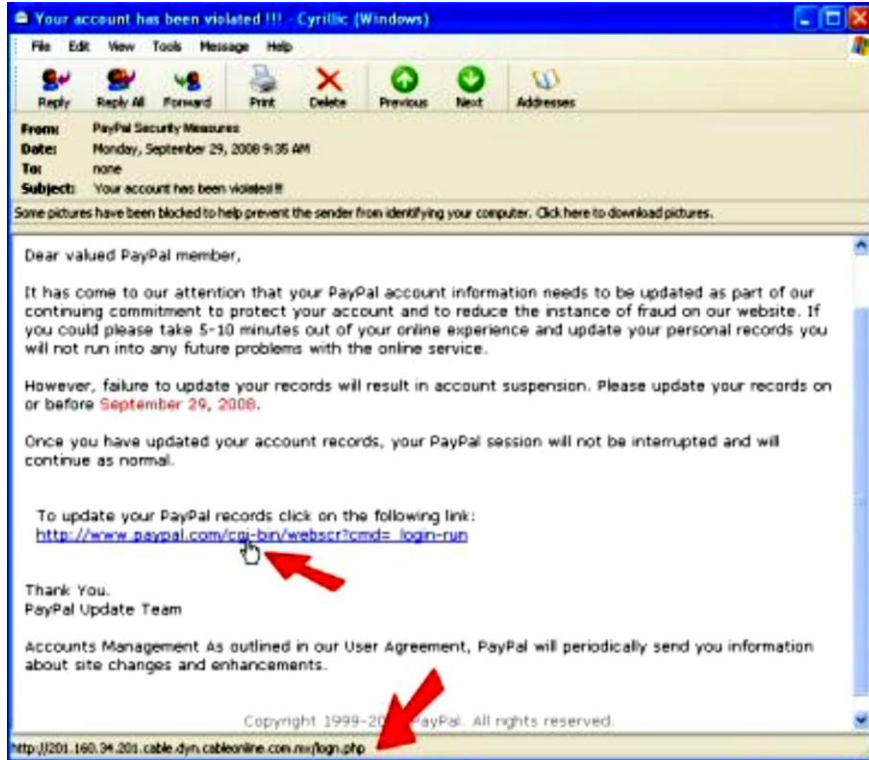
Cybercrime

Digital Underground

Cybercrime

Cybercrime- an example

Your account has been violated !!! - Cyrillic (Windows)

From: PayPal Security Measures
Date: Monday, September 29, 2008 9:35 AM
To: none
Subject: Your account has been violated !!

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

Dear valued PayPal member,

It has come to our attention that your PayPal account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before September 29, 2008.

Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal.

To update your PayPal records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
PayPal Update Team

Accounts Management As outlined in our User Agreement, PayPal will periodically send you information about site changes and enhancements.

Copyright 1999-20   PayPal. All rights reserved.

http://201.160.34.201.cable.dyn.cableonline.com.mx/logn.php

What kind of attack is it?

Cyberwar

Estonia Case

The statue that sparked the first cyber war

Struxnet

Cybersecurity Threats, Impacts & Measures

Cybersecurity

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

University of Maryland University College

Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats.

Carnegie Mellon University

Security Threats

Intrusion – Unauthorized individuals trying to gain access to computer systems in order to steal information

Virus, Worm, Trojan Horse (Malware) – programs that infect your machine and carry malicious codes to destroy the data on your machine or allow an intruder to take control over your machine

Phishing – The practice of using email or fake website to lure the recipient in providing personal information

Spyware – software that sends information from your computer to a third party without your consent

Spam – programs designed to send a message to multiple users, mailing lists or email groups

Security Risks

- Compromised Personally Identifiable Information (PII);
  - ✓ *PII data refers to name, SSN, D. Licenses, bank accounts*

- Identity Theft- computer intruders intent on stealing your personal information to commit fraud or theft

- The use of unsecure settings of Peer to Peer File Sharing applications.

- Compromised computer; A computer experiencing unexpected and unexplainable
  - Disk activities
  - Performance degradation
  - Repeated login failure or connections to unfamiliar services
  - Third party complaint of a suspicious activity

- Or a stolen or lost computer

Impact on work

Questions:

- How would you know whether an email sent to you with an attachment is free from viruses?

- How do you secure sensitive data you send via email?

- What steps would you take to secure your computer from malware?

- What does the phrase " safely manage your password" mean to you?

Security Measures

1. Safely mange your password
2. Safely manage your email account
3. Secure your computer
4. Protect the data you are handling
5. Avoid risky behavior online
6. Be aware of security guidelines, policies, and procedures
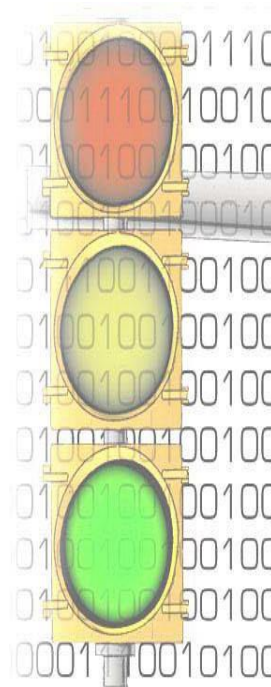
Avoid risky online behavior

- Be wary of phishing scams

- Be cautious when handling attachments and links in   email, chatrooms or instant messages (IM)

- Avoid responding to questions via pop-up windows,   or click on links in a pop-up window

- Be cautious when using Peer to Peer File Sharing   applications.

- Be cautious when browsing the web. One spelling   mistake can direct you to undesired websites

Identity Theft

Identity Theft

Identity Theft is a crime in which an impostor obtains key pieces of personal Identifying Information (PII) such as Social Security Numbers and driver's license numbers and uses them for their own personal gain.

SSN

Credit Card

NAME

DL#

Acct. #
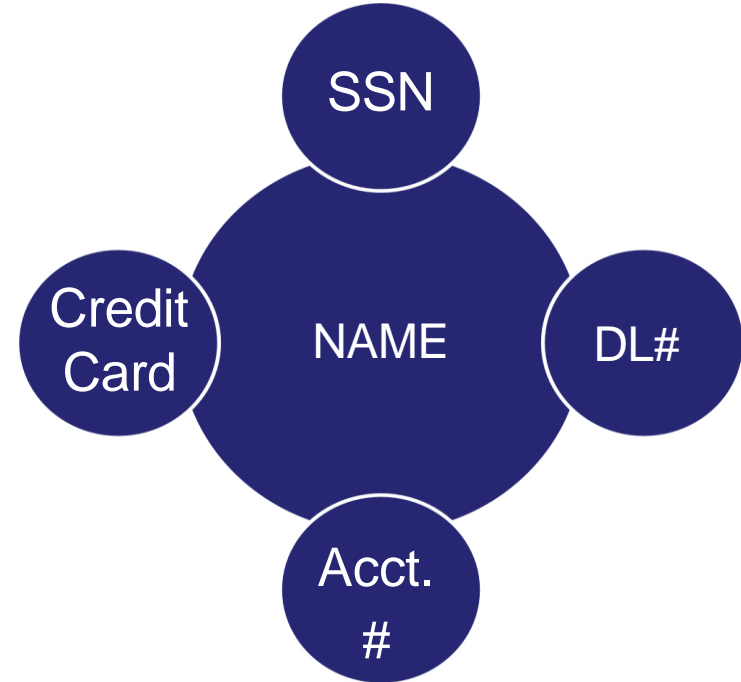
How does it happen?

- Stolen wallet
  - Driver license ID
  - Credit cards
  - Debit cards
  - Bank accounts checks; last withdrawal banking statement
  - Health insurance
  - Auto registration and insurance card
  - Frequent flyer card
- Pilfered mail
- Computer virus
- Phishing and Social Engineering
  - Links to fraudulent web sites
  - Email
  - Phone call
  - Mail
- Social Networking account
- License plate
- Health records
- Financial Data

Identity Theft Related Crimes

- Check fraud

- Credit card fraud

- Financial Identity Theft

- Criminal identity theft

- Governmental identity theft

- License plate number identity theft

- Mortgage fraud

Identity Theft Hits Close to Home

This is my street.
1 out of every 33 people means someone on my street will have their identity stolen this year.

How to protect?

- secure your mail box with a lock and make sure mail is cleared regularly
- shred or destroy your personal and financial papers before you throw them away, or keep them in a secure place if you wish to retain them
- always cover the keypad at ATMs or on EFTPOS terminals when entering your PIN, and be aware of your surroundings— is anyone trying to observe or watch you, are there any strange or loose fixtures attached to the machine or terminal?
- ensure that the virus and security software on your computers and mobile devices is up-to-date and current
-
-

Summary

We have studied

- Security

- Cybersecurity

- Cyberspace

- Cybercrime

- Identity theft

- Countermeasures

Next Week

Threats, Vulnerabilities & Attacks

Questions?