



Computer Security

What is Computer Security?

- is a branch of computer technology
- known as “*Information Security*”
- applied to computers and networks
- the objective is to protect information and property from theft, corruption, or natural disaster



Risks & Threatening

- Malware



- Social Engineering



Malware

Consists of programming designed to:

- disrupt or deny operation
- gather information that leads to loss of privacy or exploitation
- or gain unauthorized access to system resources



Examples of Malware

- Virus
- Trojans
- Bots and botnets
- Spyware

Virus

- programs that alter the functioning of our computer without our knowledge obtaining or destroying information
- spread by direct contact or sharing the same medium



Trojans

- viruses disguise as programs that supposedly do something but actually open a door on our computer so it can be accessed from outside
- his name comes from *The Trojan Horse*



Bots or Robots

- is a type of trojan that use our computer to connect to other infected computers (***zombies***)
- the goal is create ***botnets*** or ***zombie networks***
- enables to send mass mailings without be detected



Spyware

- collects small pieces of information about users without their knowledge
- search for email address, IP address, pages visited,...
- the presence of spyware is typically hidden from the user and can be difficult to detect

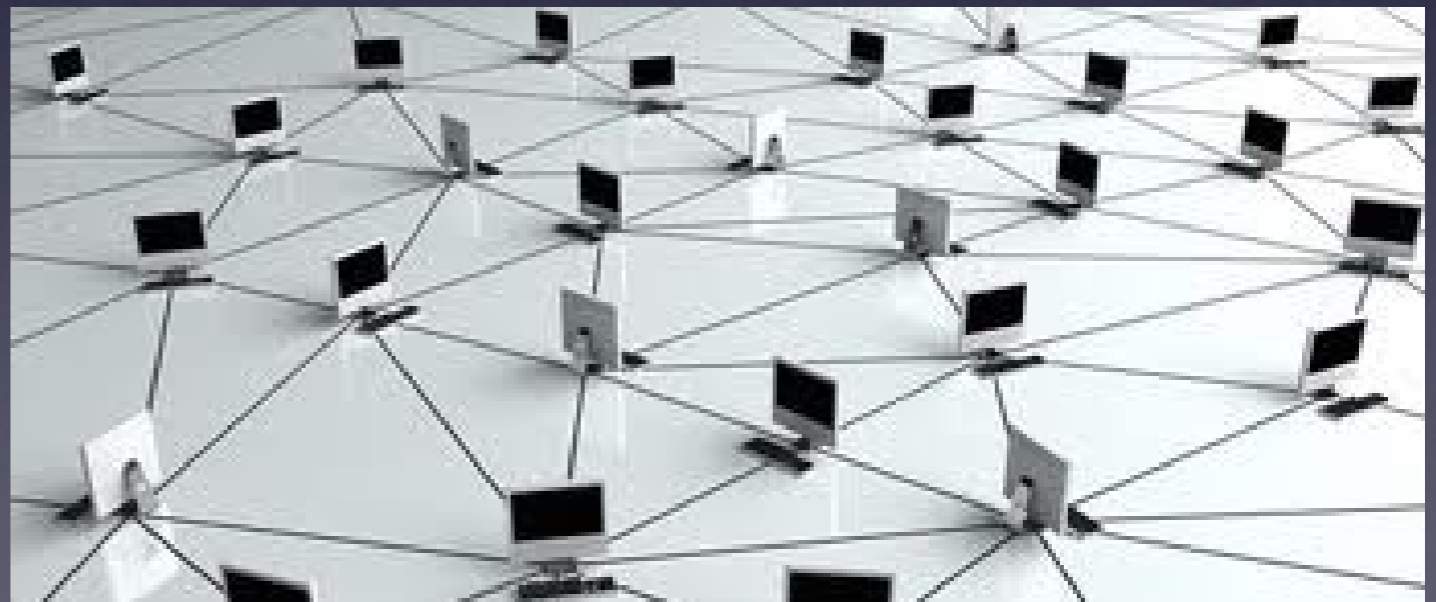


What is the propose?



How to get money?

- **directly:**
getting our bank access:
phising
- **indirectly:**
renting zombie networks
for illegal purposes



Social Engineering

- The art of manipulating people into performing actions or divulging confidential information.



Examples of Social Engineering

- Spam
- Hoax
- Phishing

Spam

- is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately
- the most widely recognized form of spam is e-mail spam



Shoulder
Pork
hAM

Hoax

- is a message warning the recipient of a non-existent computer virus threat
- the message is usually a chain e-mail
- are usually harmless



Phishing

- a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication



HowTo defend against Social Engineering?

"If something seems too good to be true, it probably isn't"

- don't share relevant information
- ensure that access the site you want
- change the password regularly

Safe Passwords

There are two rules to enforce good passwords:

- easy to remember
- not a word in the dictionary



Safe Passwords

How to create passwords easy to remember

- find a personal “*algorithm*” for generating obscure passwords
- use sayings, poems or famous quotes

Safe Passwords

Example:

**Kill Two Birds With One
Stone**

take the first letter of each word and change the numbers in

figures:

K ___ 2 B ___ W ___ 1 S ___

“k2bw1s”

Safe Passwords

Other
examples:

“2habt1”

Two Heads Are Better Than One

“1ysm7yw”

One year's seeding makes seven years weeding

“2icb3iac”

Two is company but three is a crowd

“abithiw2itb”

A bird in the hand is worth two in the bush

“str&stc”

Spare the rod and spoil the child

“w&pup4ure”

Walnuts and Pears You Plant For Your Ears