CYBER SECURITY

Presented By:
Mohammed K. Hussein

Supervised by:
Dr. Bashar M. Nema

TO UNDERSTAND

- What is the meaning of the word CYBER And Cyber space & Cyber Security
- What is the need of Cyber Security And What is Cyber Crime
- How to implement and maintain Security of a Cyber field around us.

INTRODUCTION

- The term cyber security is used to refer to the security offered through on-line services to protect your online information.

- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also.

MEANING OF THE WORD CYBER

- It is a combining form relating to information technology, the Internet, and virtual reality.

CYBER SPACE

- **Cyberspace** is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.
- actually , cyberspace can be thought as the interconnection of human beings through computers and telecommunication, without regard to physical geography.

WHAT IS CYBER SECURITY?

- **Cyber security standards** are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

- Though, cyber security is important for network, data and application security.

NEED OF CYBER SECURITY

- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses

MAJOR SECURITY PROBLEMS

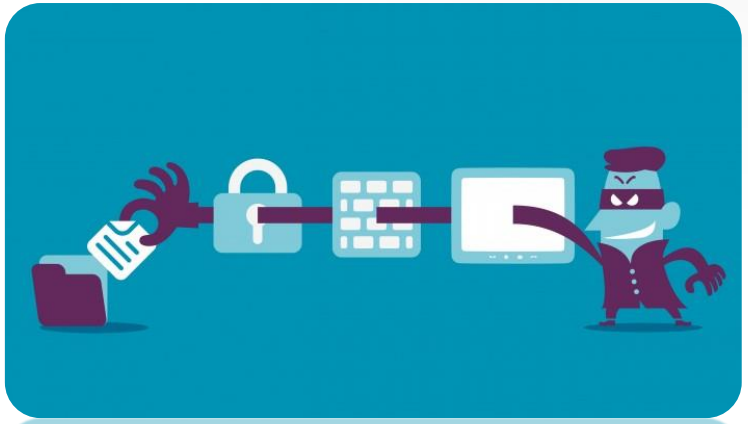
1. **Virus** is a “program that is loaded onto your computer without your knowledge and runs against your wishes
2. **Hacker** In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls (**White Hat Hacker, Grey Hat Hacker, Black Hat Hacker**) .
3. **Malware** is any software that infects and damages a computer system without the owner's knowledge or permission.
4. **Trojan horses** Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
5. **Password cracking** Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

THREATS IN CYBERSPACE

- Cyber Spyware
- Cyber terrorism
- Cyber war
- Cyber crime

CYBER SPYWARE

- **Cyber spying**, is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, of classified nature), from individuals, rivals, governments and enemies for personal, economic, political or military advantage using methods on the Internet.



For example pop-up ads as a simple spyware or any other type of virus .

CYBER TERRORISM

- is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation
- Cyber terrorism is the use of Internet based 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.
- For example A Cyber Terrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. ...Much of the same can be done to the rail lines.

CYBER WAR

- Cyber war involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through.

for example, **computer viruses** or **denial-of-service attacks** In computing, a denial-of-service attack (DoS attack) or **distributed denial-of-service attack** (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of (DoS) attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

- A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a **botnet**) flooding the targeted system with traffic. **A botnet** is a network of **zombie computers** programmed to receive commands without the owners' knowledge. When a server is overloaded with connections, new connections can no longer be accepted

- The major **advantages to an attacker** of using a distributed (DDoS) denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine

CYBER CRIME

- A computer crime refers to any illegal activity that involves a network and a coordinating computer. In an instance of computer crime, the computer may have been used during the actual commission of a crime, or the information latent within the computer may be the target of an attack.
- Net crime, which is a term used within the broader context of computer crime, refers more precisely to a criminal exploitation of the Internet. Issues surrounding these illegal actions, particularly those crimes within the field of copyright infringement, hacking

CATEGORIES OF CYBERCRIMES

Cyber crime encompasses a broad range of activities. Generally, however, it may be divided into two categories:

(1) crimes that target computers directly

(2) crimes facilitated by computer networks or devices, the primary target of which is independent of network or device.

CYBER CRIMES INCLUDES

- **Identity Theft:** Hackers and scammers may use fake emails to trick victims into giving up passwords and account information

- **Piracy:** Piracy is the copying and distribution of programs, movies, music or other intellectual property without permission.

- **Transaction Fraud:** A scammer may offer an item for sale through an auction site with no intention of delivering once he receives payment

- **Hacking:** illegally circumventing security to access someone else's computer system

Cybercrime by the numbers

WHY SHOULD WE CARE?

Cyber safety is a fundamental practice, required for everyone who keeps and accesses private information through a computer or the Internet. When an individual practices cyber safety, they are ensuring that their personal information (social security number, banking information and other confidential information) is not susceptible to being intercepted or tampered with by unauthorized users.

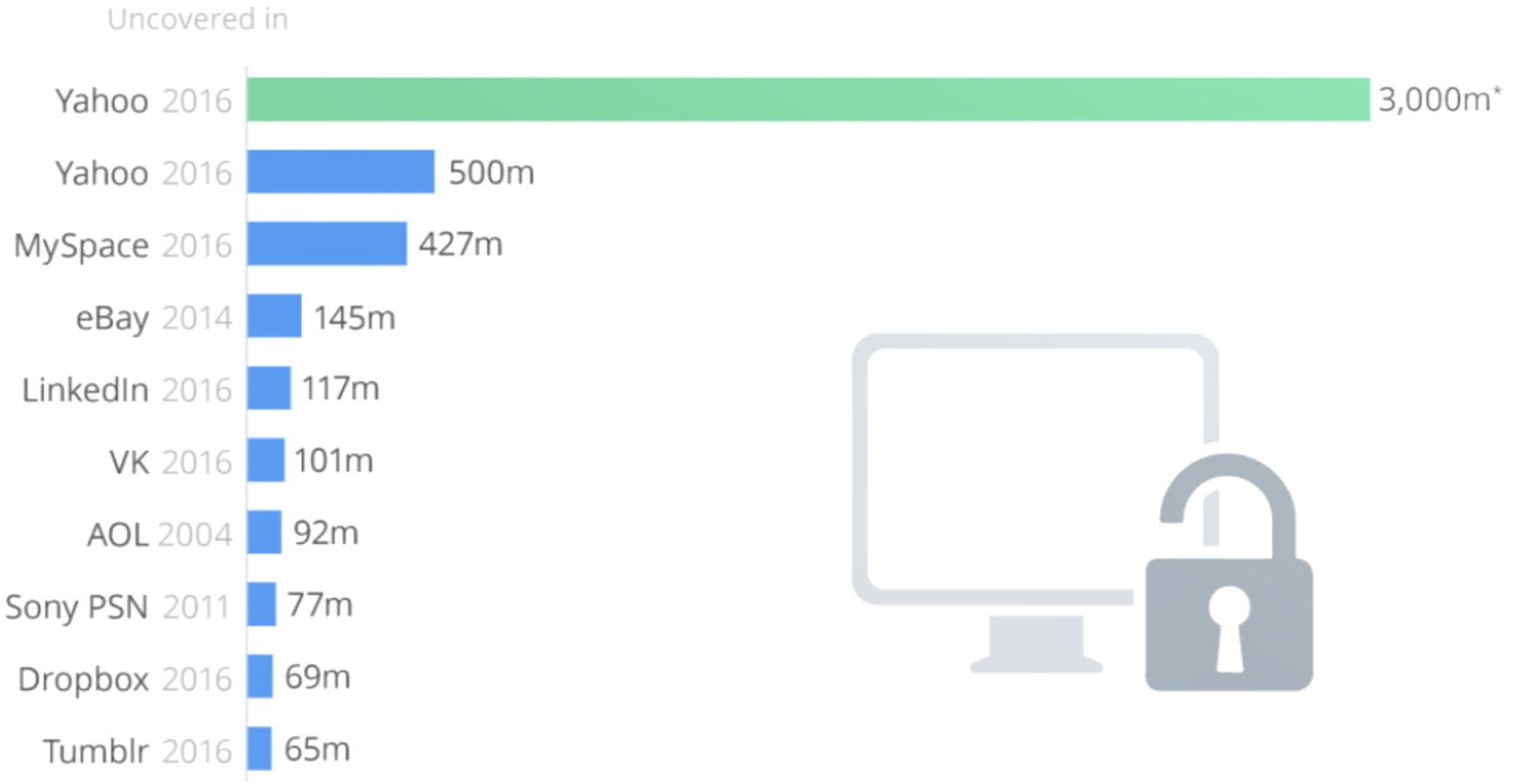
HOW CAN WE PROTECT?

- Keep your computer current with the latest patches and updates.
- Read Privacy policy carefully when you submit the data through internet.
- Encryption: lots of website uses SSL (secure socket layer)to encrypt a data.
- Choose strong passwords and keep them safe.

This Figure Show the Cyber Security Solution

3 Billion Users Affected by Yahoo Data Breach in 2013

Number of compromised accounts in selected large-scale data breaches



* when Yahoo first informed the public of the data breach in December 2016, the company estimated that the hack had affected 1 billion accounts

@StatistaCharts

Source: Media reports

statista

SUMMARY

- The term cyber security is used to refer to the security offered through on-line services to protect your online information.
- **Cyberspace** is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.
- **Cyber security standards** are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.
- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses
- **Cyber spying**, is the act or practice of obtaining secrets without the permission of the holder of the information

- Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet
- Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through.
- Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through.
- A computer crime refers to any illegal activity that involves a network and a coordinating computer.

REFERENCES

- Mark Dowd, John McDonald, and Justin Schuh," The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Addison Wesley, November 20th 2006
- Richard Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response", Starch Press, August 2nd 2013
- Michael Sikorski, and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software ", No Starch Press, February 29th 2012
- Peter Szor, "The Art of Computer Virus Research and Defense", Addison-Wesley Professional, February 13th 2005