Energiser Activity – Unit 8 e-Commerce

(These are terms we will use today – Can you find them and do you know what they are in terms of security?)

H	A	C	K	I	N	G	Y	U	O
P	A	S	S	W	O	R	D	S	P
R	T	Y	N	M	E	M	R	O	W
S	W	E	R	E	F	D	G	J	H
A	Q	L	L	A	W	E	R	I	F
D	T	Y	Y	U	I	O	P	B	N
F	R	H	J	T	R	O	J	A	N
H	T	T	P	S	R	L	G	B	N
Q	W	E	R	T	J	S	N	M	F
V	I	R	U	S	E	S	R	G	H

WORD LIST:

Hacking
Viruses
Firewall
SSL
HTTPS
RSA
Passwords
Trojan
Worm

Security

Security Risks

Aims & Objectives

Today you will learn and carry out:

- **Todays Lesson (Security Methods) P2**
- Understand what computer security is. **P2**
- What threats can you identify? **P2**
- Be able to define each security method. **P2**
- **Taking it further (Extension Activity):**
- In a brief list what countermeasures will counter security threats. **P2**

Security Threats

Types of attacks to computer security:

- Physical
  - Theft, damage, or destruction to computer equipment.
- Data
  - Removal, corruption, denial of access, unauthorized access, or theft of information.

Potential threats to computer security:

- Internal threats
  - Employees can cause a malicious threat or an accidental threat.
- External threats
  - Outside users can attack in an unstructured or structured way.

What we will cover

- **Security Risks**
- Prevention of Hacking
- Viruses
- Identity Theft
- Firewall impact on site performance

- **Protection Mechanisms**
- SSL
- HTTPS
- RSA Certificates
- Strong Passwords
- Alternative methods

Prevention of Hacking

- E-commerce sites need to prevent hacking so that the running of the business can be undisturbed and that customer details are not stolen.

- Specialist software can be used to look at all the ports on a computer and see which ports are open and closed. If a port is open and not being used that can give a hacker a way in.

- Unused ports can be protected by using a firewall.

Hacking

- There are two variations to **Hacking**:

- **Malicious** – illegal practice of an individual accessing other peoples computer systems for the sole purpose of destroying, copying or modifying data held on that computer/network. This would be for fun, spite or financial gain.

- **Ethical** – Hackers will attempt to gain access to a system and then report their unauthorised access with information on how they gained access.

Website Defacement

- **Website defacement**

  This is the most serious threat to an e-commerce organisation as an e-commerce organisation relies on its website presence to attract internet traffic and custom.

- A survey was recently done among the 400,000 recorded web server attacks. It found that 2,500 web servers each day were the victim of unauthorised access and malicious damage every day.

Website Defacement

- **Website defacement**

  Most website attacks are speculative and take advantage of weak administrative security (weak passwords or unencrypted files) or security flaws in the software itself.

- Most website defacement is done for fun. Hackers leave ‘tags’ like graffiti artists.

Website Defacement

- **Website defacement**

  Serious attacks are made for political or personal motives, either about the organisation or its services.

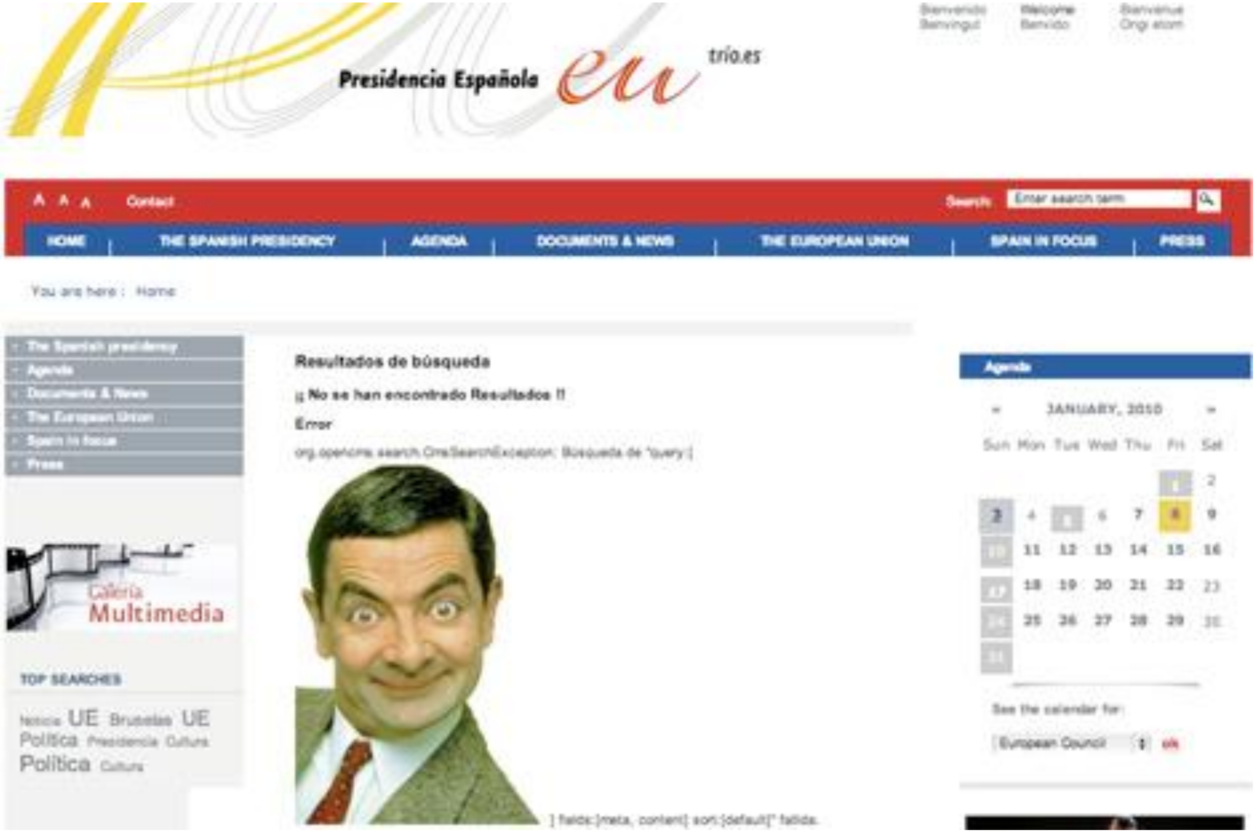
- Website defacement undermines the organisation and their professional image to their clients and potential clients.

Website Defacement

- Unidentified hackers have defaced the website of the European Union Presidency assumed by Spain at the beginning of this month. The picture of Jose Luis Rodriguez Zapatero, Spain's Prime Minister, was replaced with one depicting Mr. Bean, a world-renowned comedy character.

  (Source: http://news.softpedia.com/news/EU-Presidency-Website-Defaced-131187.shtml)

Website Defacement



Resultados de búsqueda

¡¡ No se han encontrado Resultados !!

Error

org.opencms.search.CmsSearchException: Búsqueda de "query:[ ] fields:[meta, content] sort:[default]" fallida.

Source:
http://news.softpedia.com/news/EU-Presidency-Website-Defaced-131187.shtml

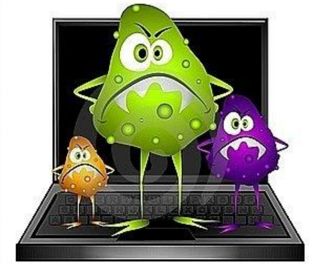
DoS (Denial of Service) Attacks

Denial of service (DoS) is a form of attack that prevents users from Accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests.

Common DoS attacks include the following:

- **Ping of death** – A series of repeated, larger than normal pings that crash the receiving computer .
- **E-mail bomb** – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

Viruses

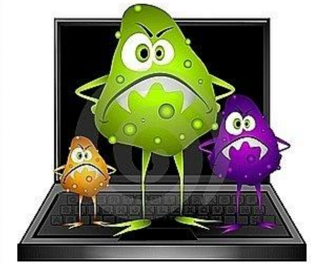


- A **computer virus** is a computer program that can copy itself and infect a computer or computer system.

- A true computer virus can only spread from one computer to another (in the form of an executable code) An example is when a user sent a virus over a network or the Internet, or carried it on a removable medium such as a USB DRIVE, CD, DVD. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

- Two examples of viruses are **Worms** and **Trojans**.

Viruses



- A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks.
- A Trojan is a program that appears harmless but hides malicious functions.
- Worms and Trojans, like viruses, may harm or damage a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and go unnoticed.

Viruses, Worms, and Trojan Horses

- Malicious software (malware) is any software designed to damage or to disrupt a system:
    - **Virus** is a software code that is deliberately created by an attacker. Viruses may collect sensitive information or may alter or destroy information.
    - A **worm** is a self-replicating program that uses the network to duplicate its code to the hosts on the network. At a minimum, worms consume bandwidth in a network.
    - A **Trojan horse** is technically a worm and is named for its method of getting past computer defenses by pretending to be something useful.
- Anti-virus software is designed to detect, disable, and remove viruses, worms, and Trojan horses before they infect a computer.

Identity Theft

- Identity Theft is not a new threat but it is one of the fasted growing crimes in the UK.
- In 2005 a survey by Which? Magazine discovered that **25%** of all **UK adults** have either had **their identity stolen** or **know** someone who has.

So how is it done?

Identity Theft

- Traditional techniques typically involve interception or theft of personal items for example:

- - Wallet/Purse/Handbag
- - Mail Deliveries
- - Discarded Bank statements, invoices, personal letters

- With this information a thief can access existing accounts, commit fraud, start loans or buy expensive items using credit agreements

Identity Theft

- As more data/information is held electronically and transferred between servers etc it is now easier than ever to use another persons identity to perpetuate such illegal acts.
- To the rescue?
- Chip and Pin/National Identity Cards

Identity Theft

- As more data/information is held electronically and transferred between servers etc it is now easier than ever to use another persons identity to perpetuate such illegal acts.

- **To the rescue?**

Chip and Pin/National Identity Cards are seen as methods which can be used to protect an Individuals identity.

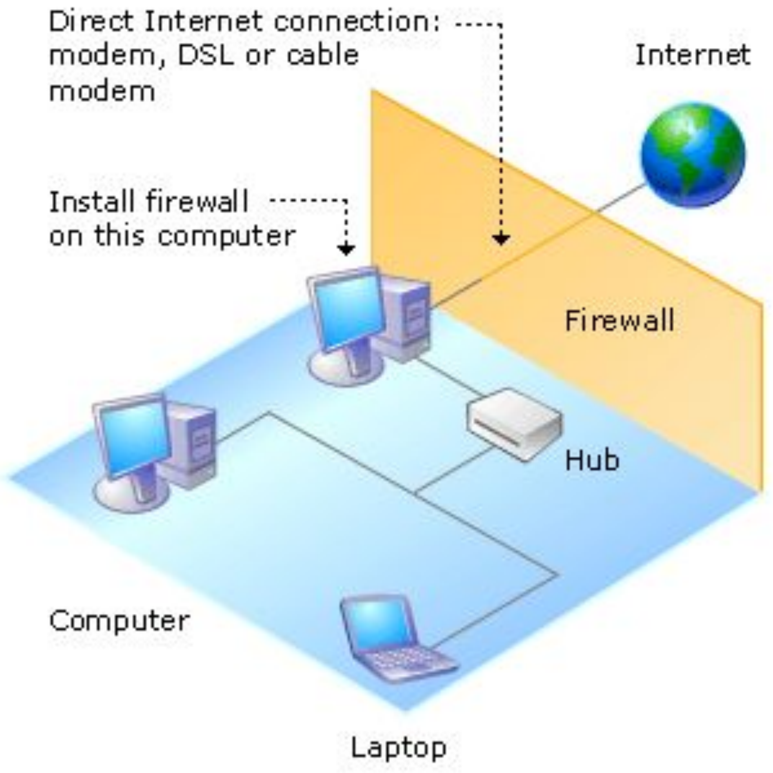
Firewalls

- A **Firewall** is a **program** which runs on a computer system (client or dedicated) that **filters network traffic**. In addition it can also specify which programs are **allowed** to access the network.

- Typically a firewall is placed **between** a **trusted private network** and an unprotected public network (such as the internet), often built into a **router** or **gateway**.

- This is done by the opening and closing of ports. Ports connect protocols and IP addresses together. Each computer has several ports for data to pass through. They are virtual so they cannot be seen. Examples of ports are Port 25 for email and Port 80 for the Internet. A web server will close all ports that are not being used.

Firewalls


Direct Internet connection: modem, DSL or cable modem
Internet
Install firewall on this computer
Firewall
Hub
Computer
Laptop

Source:
http://www.microsoft.com/middleeast/windows/windowsxp/home/using/howto/homenet/protect.aspx

Firewalls

- When using a firewall a user may not see all the features on the website. This is due to the security policies on a firewall can be set to block certain types of scripts running on a users computer.

- This is done to prevent viruses and hackers attacking the system.

- High security must be balanced with the possibility of losing functionality from websites.

Secure Socket Layers (SSL)

- SSL is a cryptographic protocol which provides secure communication on the Internet. It provides endpoint authentication which means both the server and the client need to be identified and confirm they are who they claim to be.

- This is done by public key encryption and certificate based authentication.

Secure Socket Layers (SSL)

- **Public Key**

  Is a method of coding information so only people with the right key at both ends of the communication can decode it.

- **Certificate-based authentication**
  Is a method of coding information so the people at either end are identified by a digital certificate, coupled with a digital signature. These can confirm the identity of the sender or recipient.

HTTPS

- HTTPS is the protocol usually used by websites on the Internet. HTTPS is a secure version of the protocol, which uses encryption to protect the data entered on the site.

- This protocol is usually used when customers are entering their payment details.

RSA Certificates

- RSA certificates are a method of coding information so that the people at either end are identified by a digital certificate, coupled with a digital signature.

- These can confirm the identity of the sender or recipient.

Strong Passwords

- Strong passwords are a must for all computer users. This is vital for web servers and other e-commerce systems.

- A strong password involves:

- Both letters and numbers
- Both capitals and lowercase
- Symbols such as * or #
- Being over eight characters long

Strong Passwords

- Hackers can take advantage of weak passwords especially those that are easy to guess.

- Easy to guess passwords are often the name of a pet, dates of birthdays of children or makes of cars.

- Various software programs can run through many possible combinations of characters and test each one to see if it is the chosen password. The stronger the password the longer the software will take to crack.

- Hackers are less likely to spend time attempting to hack a well secured website.

Alternative authentication Methods

- A new authentication method that is slowly becoming more popular is the use of digital signatures. These are the electronic equivalent of the traditional signatures that have been used for hundreds of years as a personal authentication method.

- A digital signature allows someone to authenticate a document over the Internet.

- An example is a customer setting up a direct debit payment would traditionally need to wait for the paperwork to be posted to them, sign it, then return it. Now digital signatures can be used to authenticate the documents immediately anywhere in the world. This benefits both the customer and businesses.

Taking it further

- **Taking it further:**

- Write a **brief report** on the below.

- In a brief list what countermeasures will counter security threats? **P2**

- What are the advantages and disadvantages of the counter measures? **P2 & M2**