GCSE OCR

Computer Science
J277

1

Network threats

Unit 4 Network security and systems software

PG ONLINE

Objectives

- Understand forms of attack and threats posed to a network:
  - Malware
  - Phishing
  - Social engineering
  - Brute force attacks
  - Denial of service attacks
  - Data interception and theft
  - SQL injection

Starter

- List at least **three** types of software that are made to harm a computer
  - How are these types of software prevented from carrying out harm?

Starter

Answers

- Harmful software includes:
  - Malware
    (viruses, worms, Trojans and ransomware)
- Prevention methods include:
  - Anti-malware, anti-virus, encryption, acceptable use policies, backup and recovery procedures

Malware

- Malware comes from two words:
  - **Mal**icious – to cause an act of harm
  - Soft**ware**
- Malware are executable programs that run on a computer
- One type of malware that exists is a computer virus
  - What are **two** other types of malware?

Malware - Viruses and worms

- Computer viruses infect computers
  - They replicate their code in other programs
  - They infect other computers
  - They harm the computer by deleting, corrupting or modifying files
- A worm replicates itself in order to spread to other computers
  - They might cause no damage to the attacked computers
  - They slow down networks and computers

Malware - Trojan horses

- During the Trojan War there is a story that the Greeks made a wooden horse and hid men inside
  - The Trojans brought the horse into the city, allowing the Greeks to open the city gates letting the army in to destroy Troy
- Computer Trojans are similar:
  - They have a program, game or cracked file which is something the user wants
  - They have negative program code which causes damage, takes control, or provides access to the computer

Malware - ransomware

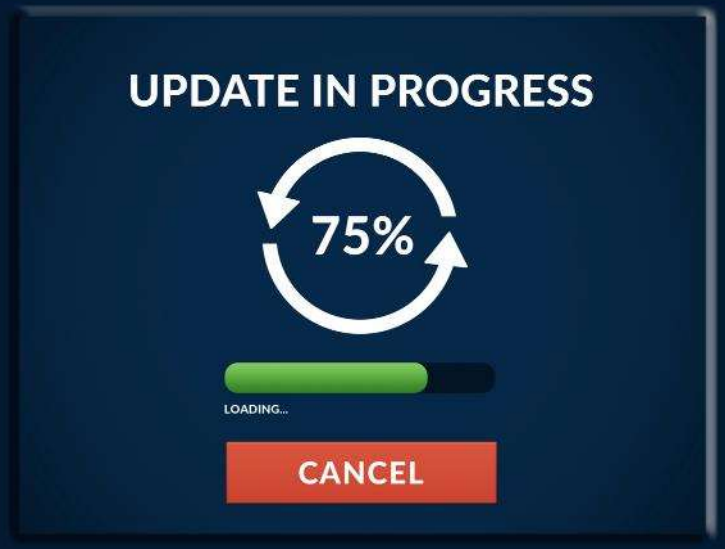
- Ransomware is software which:
  - Holds a computer hostage by locking or encrypting access to it
  - If the data is encrypted, not even a cyber security professional will be able to recover the data unless backups are available
  - Once a ransom is paid to the attacker, access is restored
- Should the ransom be paid?

Worksheet 4

- Now complete **Task 1** on **Worksheet 4**

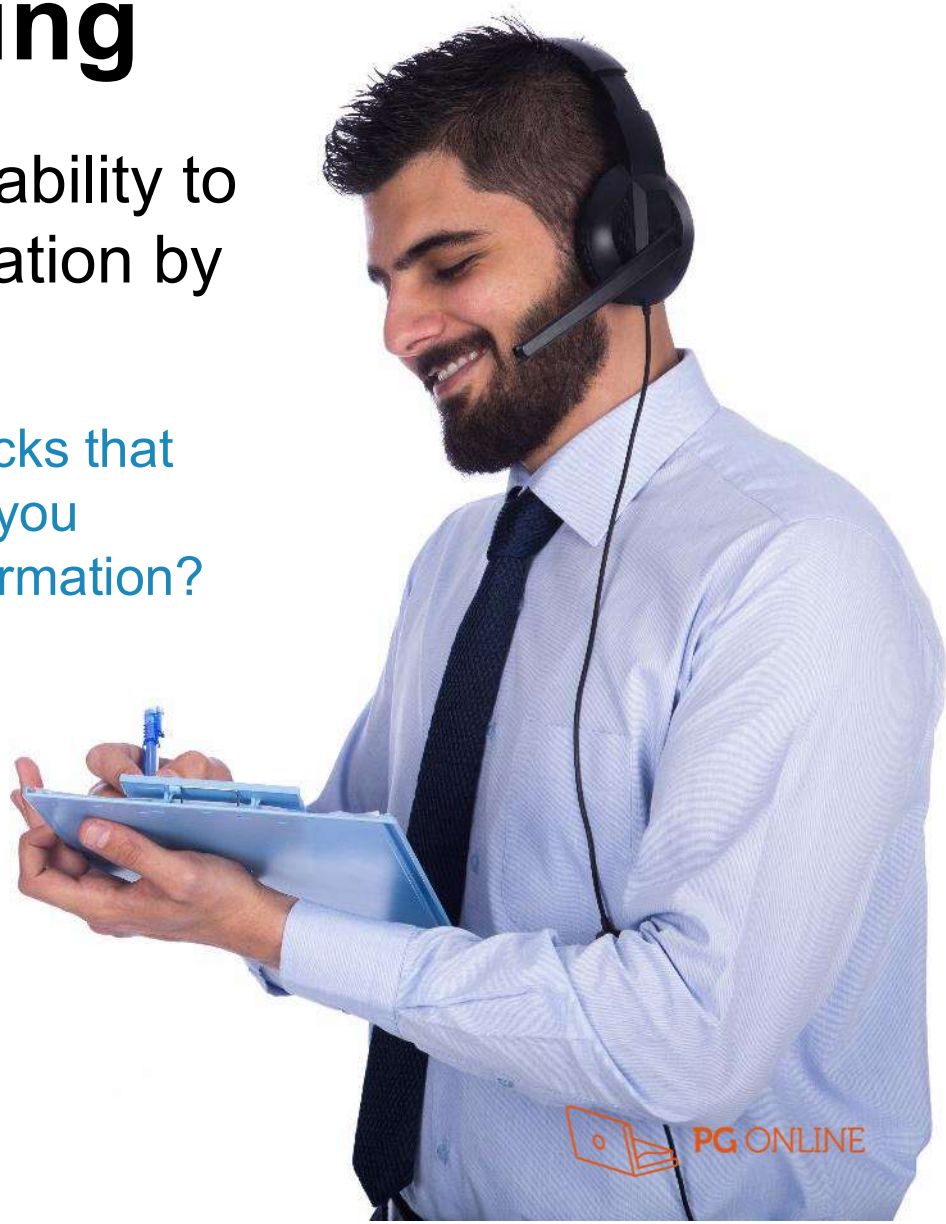
Exploiting vulnerabilities

- There are a number of ways that hackers can exploit technical vulnerabilities. Two of these include:
  - **Unpatched software** – if software updates and security updates are not installed then the software will be vulnerable
  - **Out-of-date anti-malware** – if software, such as antivirus software, isn't regularly updated then it won't be able to detect the latest viruses
- What other technique can hackers use to gain access to passwords and personal data?



Social engineering

- Social engineering is the ability to obtain confidential information by asking people for it
  - What are two confidence tricks that would get someone to give you confidential or personal information?

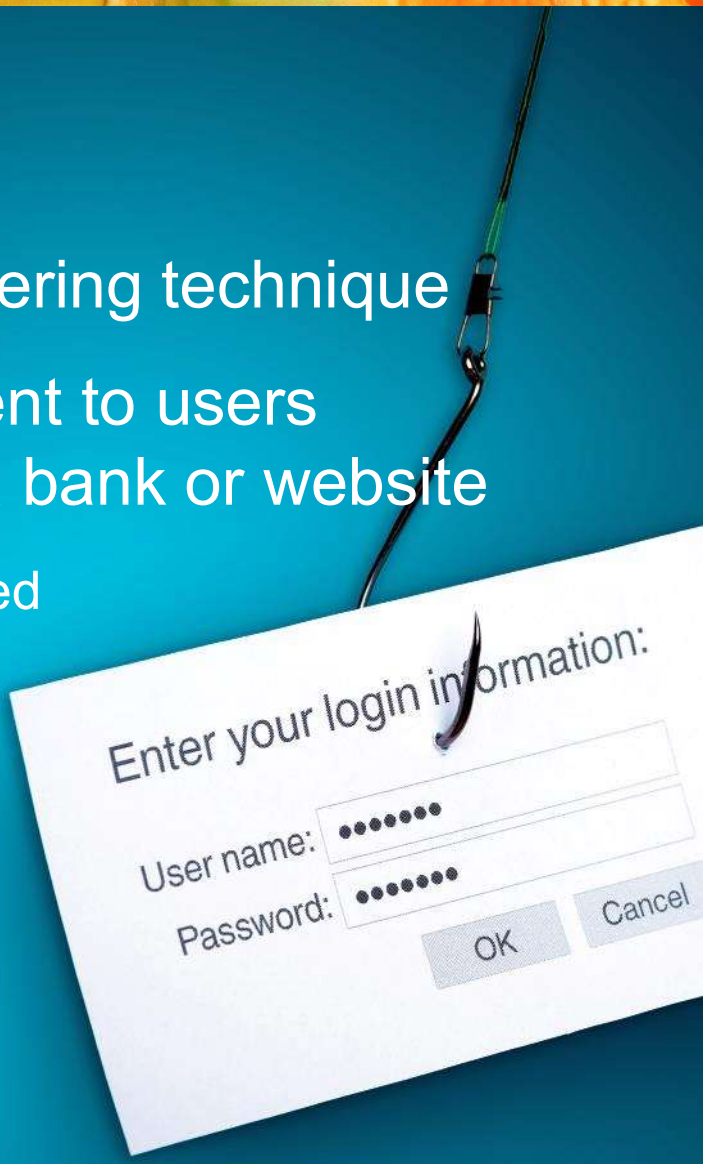


Shoulder surfing

- Shoulder surfing is the ability to get information or passwords by observing as someone types them in
- The following are two examples:
  - Looking over someone's shoulder
  - Using a CCTV camera
- What are **two** other ways that shoulder surfing could be carried out?

Phishing

- Phishing is a type of social engineering technique
- Emails, texts or phone calls are sent to users commonly pretending to be from a bank or website
  - The 'From' email address may be forged
- These messages will try to get personal information such as:
  - Usernames
  - Passwords
  - Credit cards details
  - Other personal information



A typical phishing email

Halifax Bank Plc (no-reply@home.ne.jp) Add to contacts 25/06/2014

To: Recipients

Hi,

We're just checking this is the right email address for you.
Soon your email address will become your username to access Halifax Account - that makes it easier than remembring yet another username.

If this is the email address you want to use, all you have to do is click the link below
https://my.halifax.co.uk/your-account/verify-email-details?verificationCode=eee96442-51d6-4868-b0f3-a5484447eae8
We'll let you know when your username has been changed to your email address.
If you don't verify your email address you'll need to re-register if you want to view your bill online or make change to any of your accounts in the future.

Thanks
The Online Team
Halifax

What to look out for

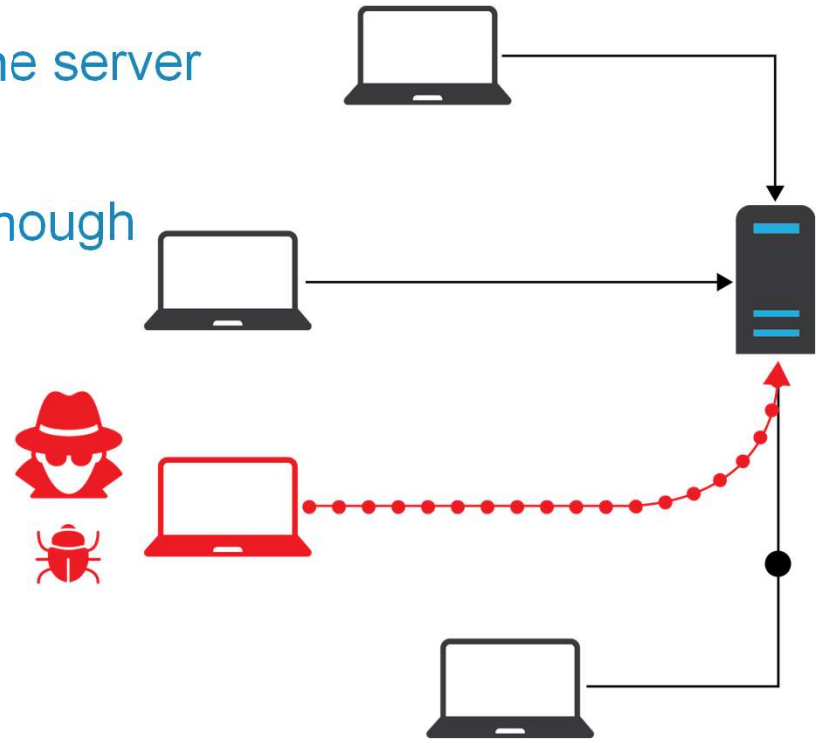
- **Greeting:** The phishers don't know your name – just your email address, so the greeting is not personalised
- **The sender's address** is often a variation on a genuine address
- **Forged link:** The link looks genuine, but it may not link to the website given. Roll your mouse over it to check
- **Request for personal information:** Genuine organisations never do this
- **Sense of urgency:** Criminals try to persuade you that something bad will happen if you don't act fast
- **Poor spelling and grammar**

Worksheet 4

- Now complete **Task 2** and **Task 3** on **Worksheet 4**

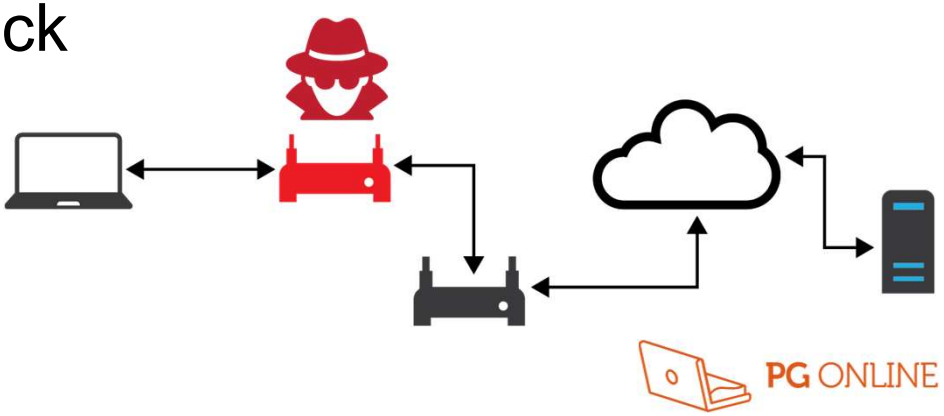
Denial of Service (DoS)

- In a denial of service attack, a hacker will use or infect a computer so that:
  - it sends as many requests to the server as it can (known as a flood)
  - the server can't respond fast enough so slows down or goes offline
- In a distributed denial of service attack (DDoS), many computers are used to send the requests



Man-in-the-middle attack

- A man-in-the-middle attack (MITM) allows the attacker to intercept communications between the user and server. The attacker can then:
  - eavesdrop to find passwords and personal information
  - add different information to a web page or other communication such as email
- Connecting to unencrypted Wi-Fi makes it easy to perform a MITM attack



Found – a free USB stick!

- Criminals sometimes leave a USB stick containing malware in a public place such as a company car park
  - An unsuspecting employee may pick it up and insert it into their computer
  - The malware can now install onto the computer so that a hacker can gain access to files, personal data and system resources

Data theft

- In 2014, the details of 125,000 students of Staffordshire University were stolen from a laptop left in a car
  - Data included the address, telephone number and email addresses for university applicants since 2006
  - Where could this information end up?
  - How could it be used?

Threats from digital devices

- Digital devices are often targeted by criminals
  - Loss of a mobile phone can lead to the loss of all the data stored on it, including passwords, account numbers and credit card details
  - Malware which targets digital devices may create ‘back doors’ to give malicious users access to your device
  - Many apparently legitimate apps are malicious and may lead to fraudulent charges on your phone bill or theft of personal information
- How can these risks be reduced on a mobile phone?

Protect your mobile phone

Answers

- Reducing threats on mobile devices
  - Use the password feature and choose a strong password
  - Make sure the data is encrypted
  - Do not follow links in suspicious emails
  - Think carefully before posting your mobile phone number on public websites
  - Don’t install apps without researching them first – if they require unnecessary extra permissions, don’t install them
  - Delete all information stored on your mobile before discarding

Brute force attacks

- In a brute force attack, a hacker will try every combination of password until the correct password is found
  - A computer program is usually used to do this as it can try millions of passwords per second

Password attempt	Outcome
0001	Incorrect password
0002	Incorrect password
0003	Incorrect password
0004	Incorrect password
0005	Password found

Worksheet 4

- Now complete **Task 3** and **Task 4** on **Worksheet 4**

SQL injection

- SQL (Structured Query Language) is a database query language
- SQL injection takes advantage of web input forms to access or destroy data
  - SQL commands can be input into web forms instead of the expected ‘real’ data
  - This can be interpreted by vulnerable web applications and end up causing damage or releasing personal information

Web form SQL

- The following line of SQL may be used in conjunction with a web form to display product data:

```
txtProductId = getRequestString(“ProductId");

SELECT *
FROM Product
WHERE ProductId = " + txtProductId;
```

Product Id: [ ] Display data

Injecting SQL

- Entering '*00237*' as the Product ID would update the criteria in the SQL and display all of the record data for that product for example:

```
WHERE ProductId = 00237;
```

Product ID	Name	Description	Price	Manufacturer	Availability
00237	Small Tiger	Soft toy	11.99	StripeyToys	In stock

- Entering '*00237; DROP TABLE Customers*' adds an SQL command to delete all company customer data:

```
WHERE ProductId = 00237; DROP TABLE Customers
```

Worksheet 4

- Now complete **Task 5** on **Worksheet 4**

Plenary

- In a pair, come up with one accurate sentence to describe each of the following forms of attack:
  - Malware
  - Phishing
  - Social engineering
  - Brute force attacks
  - Denial of service attacks
  - Data Interception and theft
  - SQL injection

Plenary

Answers

- Malware – software that aims to harm computers and/or data
- Phishing – emails that pretend to be from legitimate companies but actually try to gain personal information
- Social engineering – deception to gain personal information
- Brute force attacks – trying all possible passwords until the correct one is found
- Denial of service attacks – flooding a server or network with pointless requests so that it fails or slows down
- Data Interception and theft – stealing data or intercepting it with a man-in-the-middle attack
- SQL injection – using web forms to add SQL instructions to a query that cause data loss or the revealing of personal information

Copyright

Licence agreement