

GCSE OCR

Computer Science
J277

2

Identifying and preventing vulnerabilities

Unit 4 Network security
and systems software



PG ONLINE

Objectives

- Identify and understand the prevention of vulnerabilities including the use of:
 - penetration testing
 - anti-malware software
 - firewalls
 - user access levels
 - passwords
 - encryption
 - physical security

Starter

- Computers are vulnerable to many threats such as:
 - Malware including viruses
 - Social engineering
 - Denial of service attacks
 - Brute-force attacks
 - Data interception
- What methods do you use at school or home to reduce the risk of these threats?



Preventing vulnerabilities

Answers

- There are many ways that vulnerabilities are protected against – in particular:
 - penetration testing
 - anti-malware software – including anti-virus software
 - firewalls
 - user access levels
 - passwords
 - encryption
 - physical security



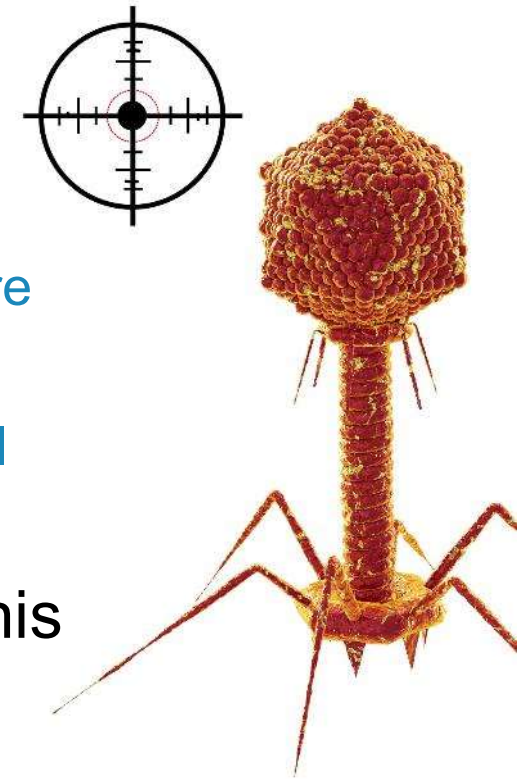
Penetration testing

- 'Pen' testing is the practice of deliberately trying to find security holes in your own systems
- The goal of penetration testing
 - identify the targets of potential attacks
 - identify possible entry points
 - attempt to break in
 - report back the findings



Anti-malware software

- Anti-malware software will detect malware such as viruses, worms, trojans, and spyware
 - When a virus or new malware is detected it is sent to the anti-virus company
 - They verify it is malware then create a signature of the virus
 - They then add it to their virus database and tell computers to run an update
- Viruses can morph to avoid detection. This makes it harder to create a signature

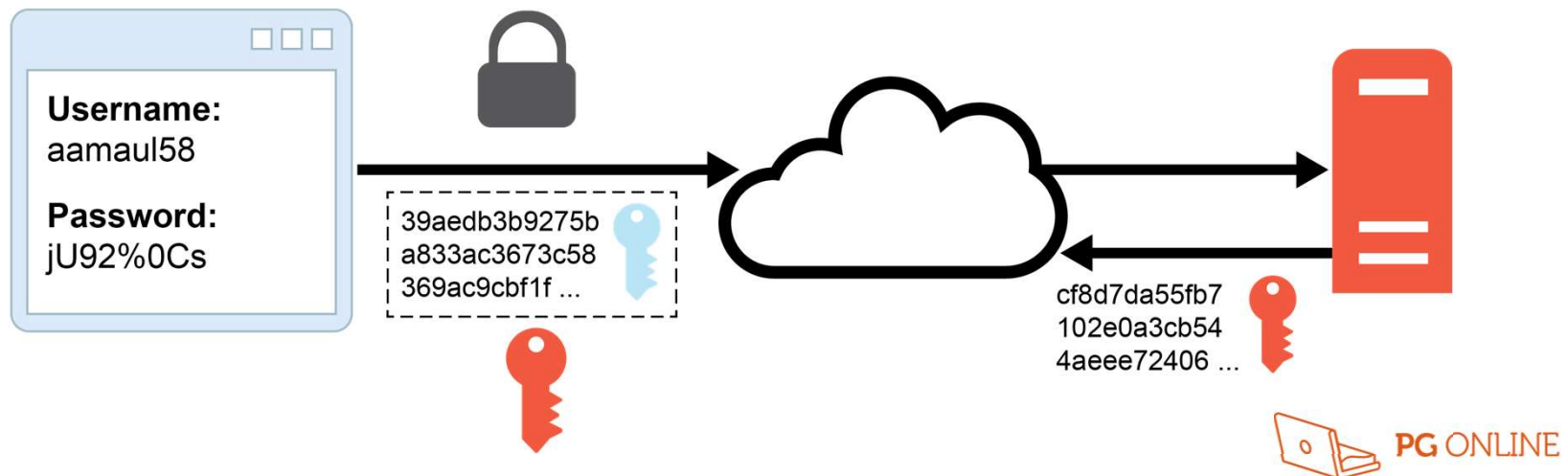


Encryption

- Encryption is a way of securing data so that it cannot be read without the encryption key
 - Passwords stored by websites are almost always stored in an encrypted form
 - If a hacker obtains the data in the password database, they won't be able to easily read the passwords
 - Devices and computers can also have their storage and hard disk data encrypted
- How do you know if a website you are using is encrypting the communication between your computer and the website?

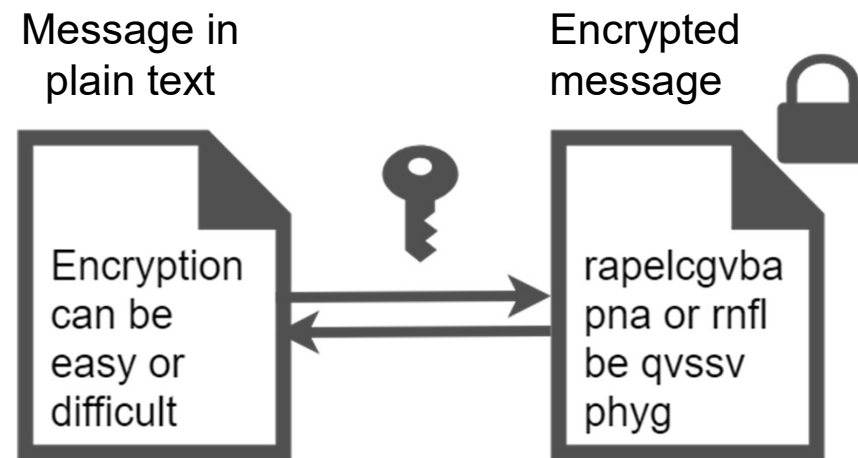
Encryption of transmitted data

- Websites using HTTPS (Secure HyperText Transfer Protocol) encrypt the connection to the server
 - Your web browser sends its key and form data, encrypting it with the server's key
 - The server encrypts the web page you request using your web browser's key



Encryption of individual files

- Files can be encrypted individually on a computer using a password
- They can then only be viewed by people who have the password
- Software such as zip files allow encryption to be applied
 - The message on the right uses a very simple encoding. How does it work?



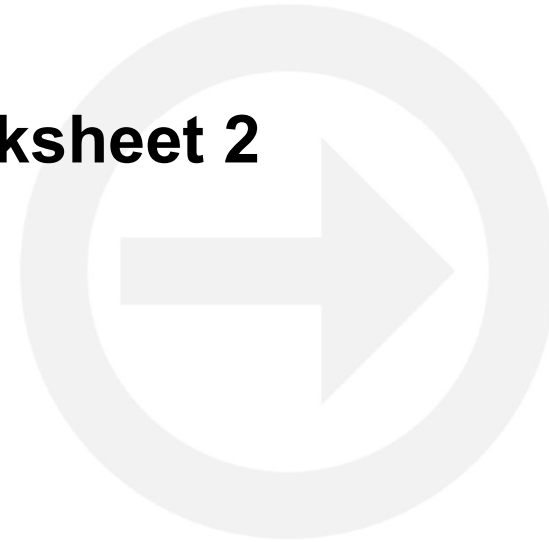
Encryption of drives

- Ordinary computer drives can be encrypted so that a password is needed to access the information
 - This prevents a hacker from removing a hard drive and installing it to a different computer to read its contents
- For removable media, special hardware can be purchased which encrypts data on the disk



Worksheet 2

- Now complete **Task 1** on **Worksheet 2**

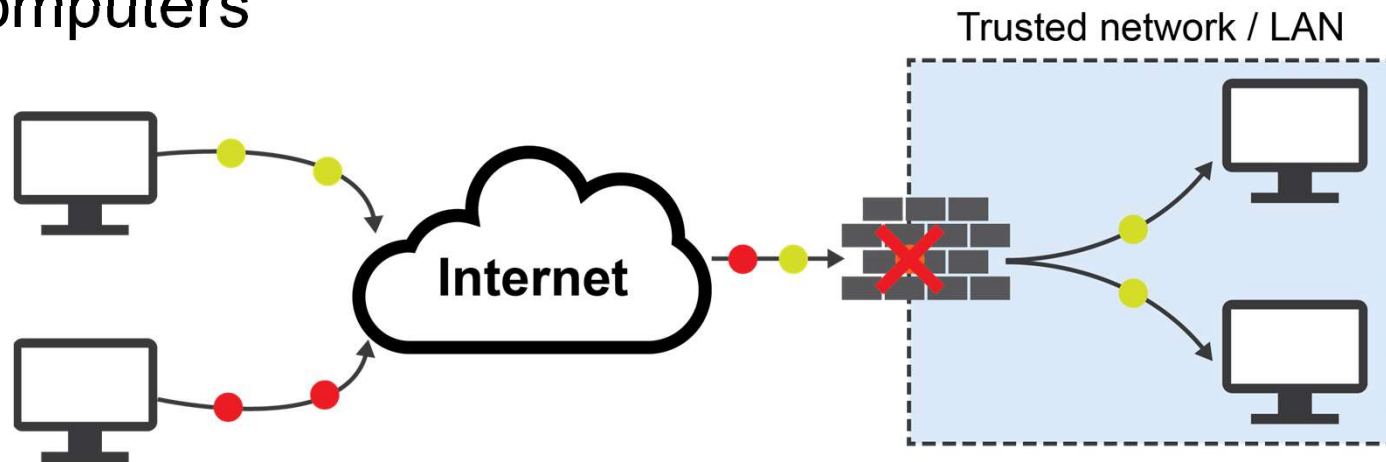


Firewalls

- Separate a trusted network from an untrusted network (normally the Internet)
- Data is sent around a network in small packets of information
- These packets are checked to see where they are coming from and going to
 - Packets that don't match filtering rules are dropped
 - This is known as a packet filter
- Firewalls can be run on dedicated hardware or as software

Firewalls

- Firewalls may be built into your hardware
 - This may be a dedicated unit to the task of being a firewall
 - Alternatively, it may be built into other devices such as a home Wi-Fi router
- The firewall will detect packets from malicious computers

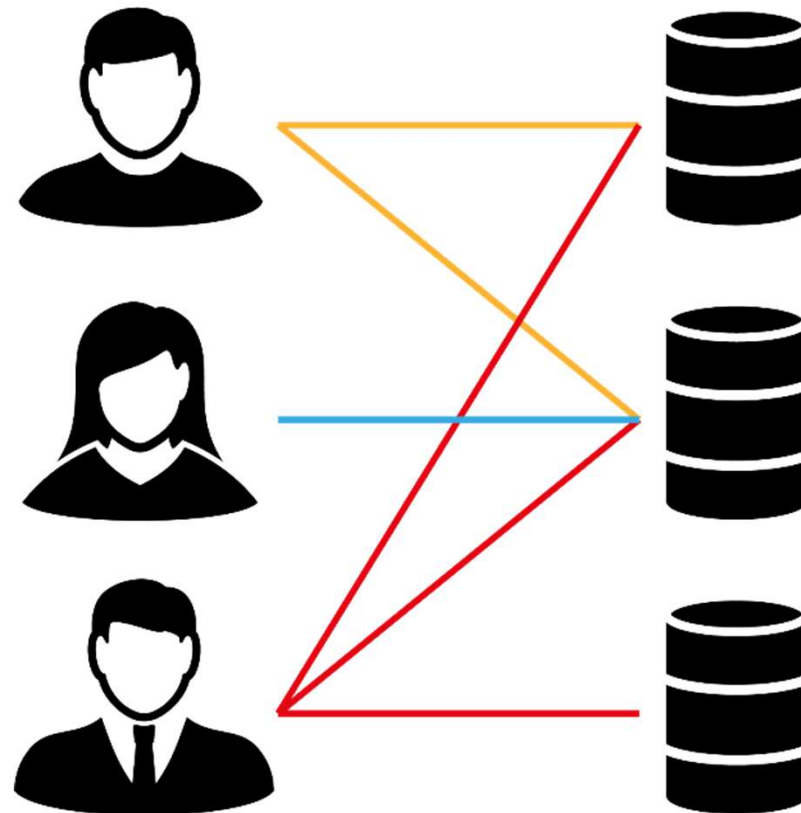
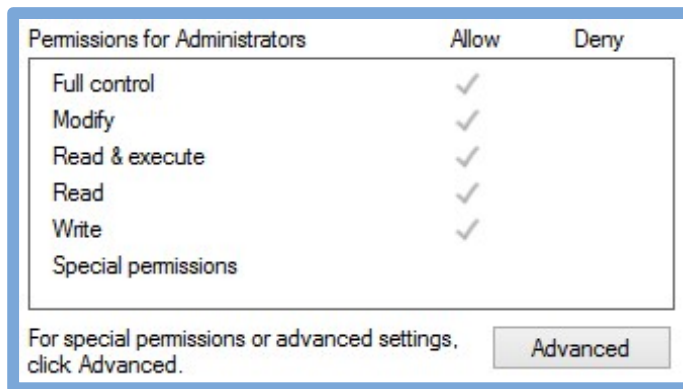


Firewall capabilities

- Firewall features:
 - Prevents attackers from gaining access to computers on a network
 - Can block certain malicious computers by filtering packets from a certain IP (Internet Protocol) address
 - Can prevent access to certain ports on the network. This is known as port blocking
 - Malicious or inappropriate websites can be blocked
 - Dedicated hardware firewalls are expensive
 - Software firewalls will slow down a computer

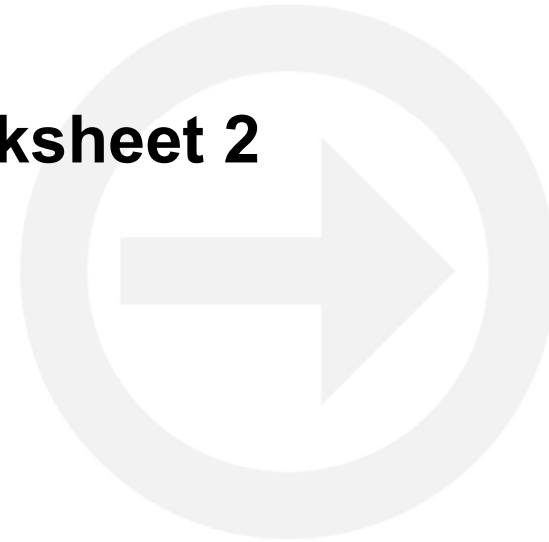
User access levels

- Access rights may be set on disks, folders and even individual files
 - How are access rights used in school?



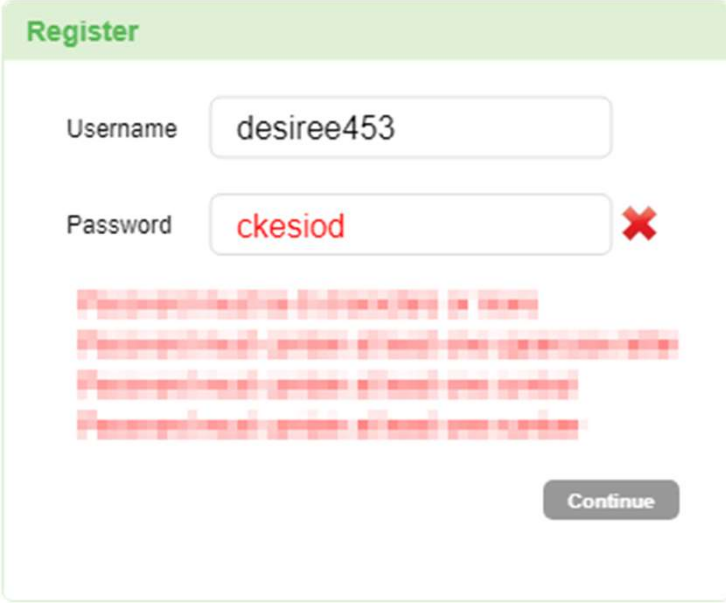
Worksheet 2

- Now complete **Task 2** on **Worksheet 2**



Password policy

- Passwords are often checked as they are created to make sure that they conform to the parameters given in a required policy
 - Four error messages have been given for this password. What are they likely to be?



The screenshot shows a registration form with the following fields and content:

- Register** (header)
- Username**: desiree453
- Password**: ckesiod (with a red 'X' icon indicating an error)
- Four red error messages (blurred text) below the password field.
- Continue** button.

Password policies

- Organisations and computer systems will often have password policies. These will make sure that your chosen password has features like:
 - Minimum length of characters
 - Include at least one lowercase letter
 - Include at least one uppercase letter
 - Include at least one symbol
 - Change password every month
- Pa55w*rd meets all the above criteria. Is it a good password?



Physical security

- Physical security is where hardware, software and networks are protected by physical methods
- An example would be security lighting
 - What are **five** other methods of physical security that are used?



Physical security

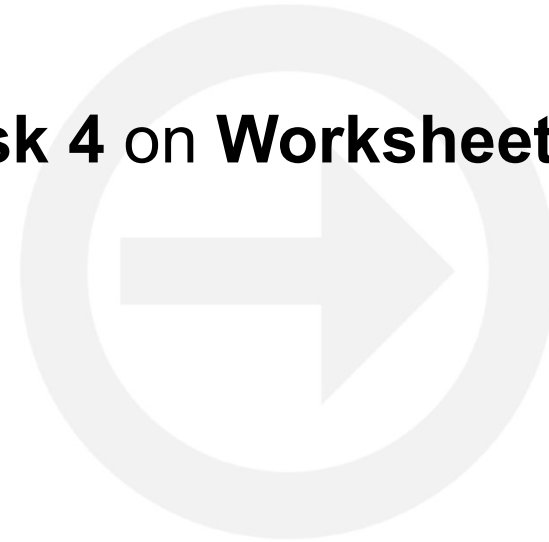
Answers

- Physical security methods include:
 - CCTV
 - Intruder alarms
 - Locks on doors or cabinets
 - Fences, walls, barbed wire
 - Security guards
 - ID cards and signs
 - Turnstiles and gates



Worksheet 4

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



Plenary

- For each of the following, state whether it is:
 - A threat to a digital system
 - A way of protecting a digital system

Viruses

Encryption

Trojans

Penetration testing

Physical security

User access levels

Anti-malware

Firewalls

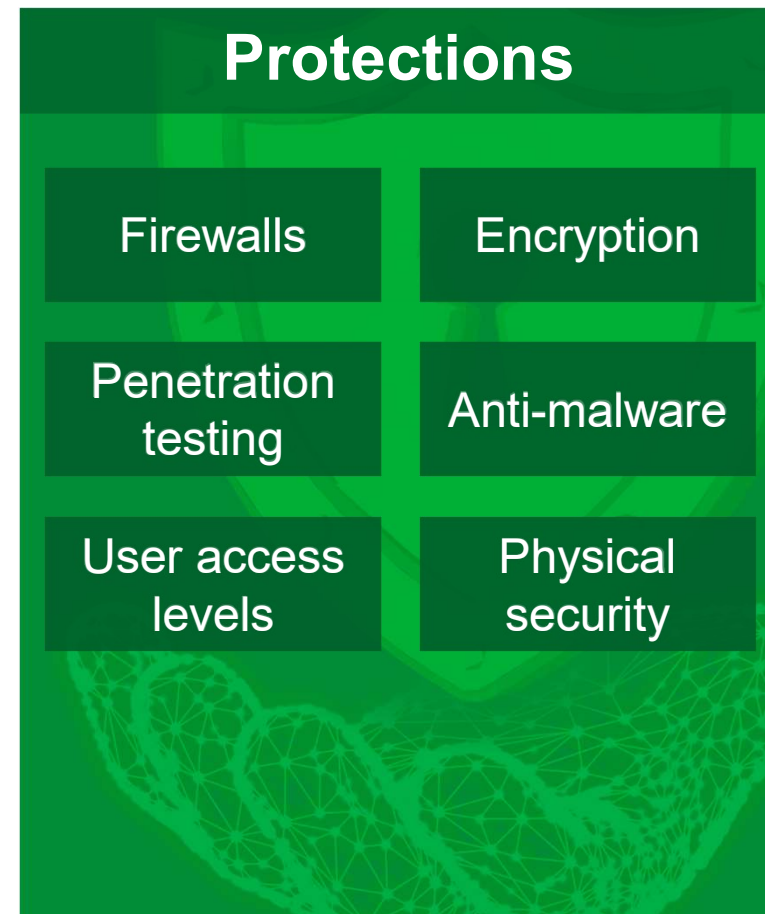
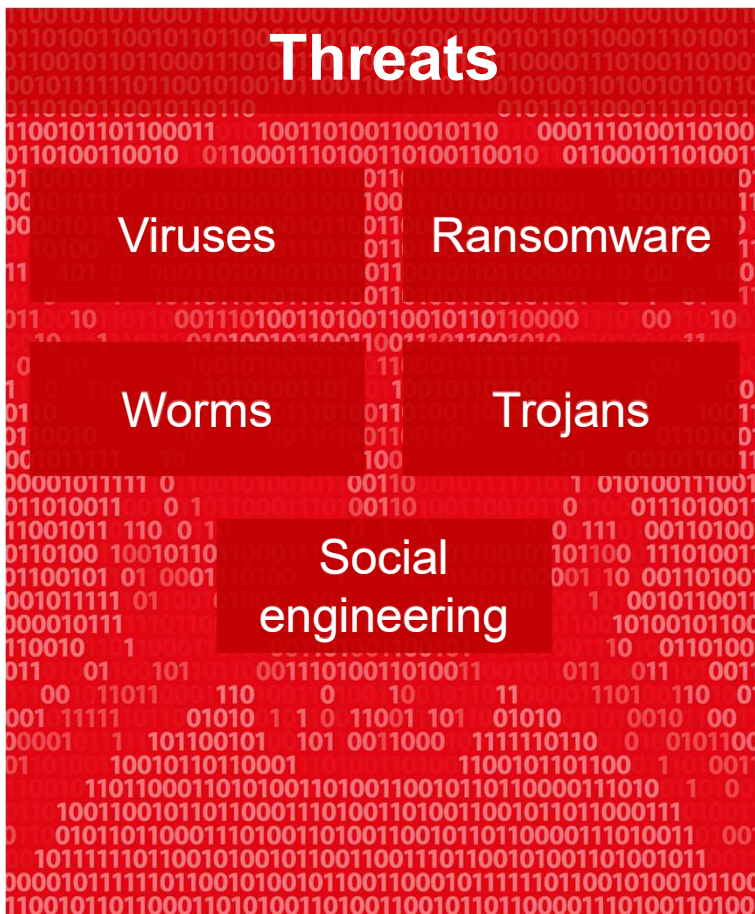
Ransomware

Worms

Social engineering

Plenary

Answers



Copyright

© 2020 PG Online Limited

The contents of this unit are protected by copyright.

This unit and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it are supplied to you by PG Online Limited under licence and may be used and copied by you only in accordance with the terms of the licence. Except as expressly permitted by the licence, no part of the materials distributed with this unit may be used, reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic or otherwise, without the prior written permission of PG Online Limited.

Licence agreement

This is a legal agreement between you, the end user, and PG Online Limited. This unit and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it is licensed, not sold, to you by PG Online Limited for use under the terms of the licence.

The materials distributed with this unit may be freely copied and used by members of a single institution on a single site only. You are not permitted to share in any way any of the materials or part of the materials with any third party, including users on another site or individuals who are members of a separate institution. You acknowledge that the materials must remain with you, the licencing institution, and no part of the materials may be transferred to another institution. You also agree not to procure, authorise, encourage, facilitate or enable any third party to reproduce these materials in whole or in part without the prior permission of PG Online Limited.