Computers

VOCABULARY PRACTICE

UPPER-INTERMEDIATE | B2

Name: _____ **Date:** _____

1 Match each digital-system term with its meaning.

1 cloud computing	____	a deceptive attempt to obtain confidential information
2 bandwidth	____	b original human-readable instructions behind a program
3 encryption	____	c unauthorised exposure of protected information
4 firewall	____	d harmful software designed to damage or exploit systems
5 malware	____	e visual controls through which a person uses a system
6 phishing	____	f delivery of computing resources over the internet
7 data breach	____	g software whose code may be inspected and modified
8 user interface	____	h system that filters incoming and outgoing network traffic
9 source code	____	i process of converting information into protected form
10 open-source software	____	j amount of data a connection can transmit in a given time

2 Complete the cybersecurity collocations.

access | **breach** | **credentials** | **encrypt** | **patch** | **permissions** | **traffic** | **vulnerability**

1 detect a security _____

2 steal login _____

3 _____ sensitive data

4 restrict user _____

5 apply a software _____

6 monitor network _____

7 gain unauthorised _____

8 exploit a _____

3 Choose the most precise term for the context.

1 Remote servers provide processing and storage: *cloud computing / bandwidth*.

2 A fake login page captures passwords: *phishing / malware*.

3 A filter blocks suspicious connections: *firewall / interface*.

4 Protected text is unreadable without a key: *encryption / source code*.

5 Attackers publish customer records: *data breach / open source*.

6 A slow connection cannot carry enough data: *bandwidth / permissions*.

7 Users navigate through menus and buttons: *user interface / firewall*.

Computers

4 Complete the incident report with terms from the box.

access | bandwidth | credentials | data breach | encryption | firewall | malware | phishing | source code | vulnerability

An employee entered login **1** _____ on a convincing **2** _____ page. Attackers used them to gain **3** _____ and install **4** _____. They exploited a known **5** _____ in old **6** _____. Although the **7** _____ blocked some traffic, the incident caused a **8** _____. Stronger **9** _____ limited exposure, while extra network **10** _____ helped the recovery team transfer backups quickly.

5 Read the text and answer the questions briefly.

Designing secure access

A charity replaced shared passwords with individual accounts and multi-factor authentication. Staff received only the permissions required for their roles. Administrators recorded unusual login attempts and reviewed access when employees changed jobs. The measures reduced risk, but they also created friction for volunteers using older phones. The charity therefore offered security keys and short training sessions rather than weakening the controls.

1 What replaced shared passwords? _____

2 How were permissions limited? _____

3 What activity did administrators record? _____

4 When was access reviewed? _____

5 What practical problem did volunteers face? _____

6 How did the charity respond without weakening security? _____

6 Rewrite using the expression in capitals.

1 Someone accessed the system without permission. **UNAUTHORISED** ___

2 The information was converted into protected form. **ENCRYPTED** ___

3 The program contains a weakness attackers can use. **VULNERABILITY** ___

4 The organisation exposed protected records. **BREACH** _____

OVER TO YOU

Write a **120-150 word** security plan for a school or small organisation. Address accounts, permissions, phishing, updates, encryption, backups and user support.

[ ] Use at least ten target terms. [ ] Balance security with usability. [ ] Include prevention and response.

ANSWER KEY

1 Digital-system terms

1 **f** 2 **j** 3 **i** 4 **h** 5 **d** 6 **a** 7 **c** 8 **e** 9 **b** 10 **g**

2 Cybersecurity collocations

1 **breach** 2 **credentials** 3 **encrypt** 4 **permissions** 5 **patch** 6 **traffic** 7 **access** 8 **vulnerability**

3 Precise terms

1 **cloud computing** 2 **phishing** 3 **firewall** 4 **encryption**
5 **data breach** 6 **bandwidth** 7 **user interface**

4 Incident report

1 **credentials** 2 **phishing** 3 **access** 4 **malware** 5 **vulnerability** 6 **source code**
7 **firewall** 8 **data breach** 9 **encryption** 10 **bandwidth**

5 Reading - suggested answers

1 Individual accounts and multi-factor authentication. 2 By role. 3 Unusual login attempts. 4 When staff changed jobs.
5 Older phones caused friction. 6 It offered security keys and training.

6 Rewriting - possible answers

1 There was **unauthorised access**. 2 The information was **encrypted**. 3 The program has a **vulnerability**. 4 The organisation suffered a data **breach**.

Over to you: Answers will vary. Check threat precision, layered controls, usability and incident response.