AP CYBERSECURITY • EXERCISE SHEET

1.2 Suspicious Website Logins

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

Objective

Build the skills to answer exam questions on **password attacks** 密码攻击 and stronger **authentication** 身份验证.

You must be able to:

- identify signs of an online password attack in a log
- explain why weak, patterned passwords fail
- recommend stronger authentication: long unique passwords and **MFA** 多因素身份验证

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Signs in the log

An online password attack shows many failed logins in a short time, logins at unusual hours, or logins from unknown devices.

■ Making authentication stronger

Use long, random, unique passwords (a password manager helps), avoid names and dates, and enable multifactor authentication so a stolen password alone is not enough.

2 Practice

2.1 State two signs, visible in a log, of an online password attack. [2]

2.2 Explain why a password like `Summer2024!` is weak. [2]

2.3 State two ways to make authentication stronger. [2]

3 Exam-style questions

3.1 Which log pattern most strongly suggests an online password attack? [1]

- **A** one successful login
- **B** many failed logins in a short time
- **C** a file download
- **D** a printer coming online

3.2 Which is the strongest password? [1]

- **A** your dog's name
- **B** P@ssword!
- **C** a 16-character random string
- **D** your birthday

3.3 A company wants to reduce account takeovers.

(a) Name one authentication improvement they could require. [1]

(b) Explain how it helps even if a password is stolen. [2]

4 Go further

- work through the **1.2 Suspicious Website Logins** lesson on the **Learn** page;
- read the **Introduction to Security** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 any two of: many failed logins in a short time; logins at unusual hours; logins from unknown devices.

2.2 it follows a common pattern - word + year + symbol - that an adversary's dictionary of guesses expects.

2.3 any two of: use long/random/unique passwords; use a password manager; enable MFA.

3.1 B. a burst of failed logins signals guessing.

3.2 C. long + random + unique beats any pattern.

3.3 (a) multifactor authentication / MFA. (b) MFA needs a second factor, so a stolen password alone cannot log in.