

01	A	B	C	D	E
02	A	B	C	D	E
03	A	B	C	D	E
04	A	B	C	D	E
05	A	B	C	D	E
06	A	B	C	D	E
07	A	B	C	D	E
08	A	B	C	D	E
09	A	B	C	D	E
10	A	B	C	D	E
11	A	B	C	D	E
12	A	B	C	D	E
13	A	B	C	D	E

14	A	B	C	D	E
15	A	B	C	D	E
16	A	B	C	D	E
17	A	B	C	D	E
18	A	B	C	D	E
19	A	B	C	D	E
20	A	B	C	D	E
21	A	B	C	D	E
22	A	B	C	D	E
23	A	B	C	D	E
24	A	B	C	D	E
25	A	B	C	D	E
26	A	B	C	D	E

27	A	B	C	D	E
28	A	B	C	D	E
29	A	B	C	D	E
30	A	B	C	D	E
31	A	B	C	D	E
32	A	B	C	D	E
33	A	B	C	D	E
34	A	B	C	D	E
35	A	B	C	D	E
36	A	B	C	D	E
37	A	B	C	D	E
38	A	B	C	D	E
39	A	B	C	D	E

PRACTICE QUESTIONS

IC3 Digital Literacy

LIVING—ONLINE—IC3— DIGITAL—LITERACY— CERTIFICATION

Living Online (IC3 Digital Literacy Certification)

EDITION

Demo

QUESTIONS

9

FORMAT

Limited Edition PDF

Before you begin

What this is

9 practice questions for IC3 Digital Literacy **LIVING-ONLINE-IC3-DIGITAL-LITERACY-CERTIFICATION**, each with its answer key and an explanation. Answer a question before you read its key — the explanation is worth more once you have committed.

If something looks wrong

Send us three things and we will check it:

- the exam code, **LIVING-ONLINE-IC3-DIGITAL-LITERACY-CERTIFICATION**
- the question number
- the email address on your order

Write to **support@mometrix.net**. We reply within one business day.

QUESTION 1

SINGLE CHOICE

A user receives an unsolicited email that appears to be from their bank, asking them to click a link and verify their account credentials. Which term BEST describes this type of malicious activity?

- ☒ **A** Phishing
- ☐ **B** Spam
- ☐ **C** Spoofing the sender address only
- ☐ **D** Brute-force login attack

ANSWER A

WHY Phishing is a social engineering attack in which a malicious actor sends a fraudulent message designed to trick a person into revealing personal information such as credentials. While the email also contains elements of spoofing, the act of soliciting credentials through a deceptive link is the defining characteristic of phishing. Brute-force attacks attempt to guess passwords programmatically, and spam refers to unsolicited bulk email, neither of which captures the credential-harvesting intent.

QUESTION 2

SINGLE CHOICE

Which of the following BEST describes a person's digital footprint?

- ☒ **A** The unique trail of data a person leaves behind through their online activities
- ☐ **B** The physical distance between a user and the network server they connect to
- ☐ **C** A software program that records keystrokes on a computer
- ☐ **D** The amount of storage space a person uses on cloud services

ANSWER A

WHY A digital footprint is the record or trail left by the things a person does online, including websites visited, emails sent, and information submitted. The other options describe unrelated technical concepts: latency/distance, keystroke logging (a type of malware), and cloud storage capacity.

QUESTION 3

MULTIPLE CHOICE

Which of the following are examples of safe practices when using social networking sites? (Choose two.)

- ☒ **A** Adjusting privacy settings so that posts are visible only to approved contacts
- ☐ **B** Sharing your home address publicly to invite friends to a party
- ☐ **C** Accepting friend or connection requests from people you do not know without reviewing their profile
- ☒ **D** Using a unique, strong password for each social media account

ANSWER A • D

WHY Configuring privacy settings and using unique, strong passwords are well-established safe practices that limit exposure and protect accounts. Sharing your home address publicly reveals sensitive personal information, and accepting unknown contacts can expose you to social engineering and malicious actors.

QUESTION 4

SINGLE CHOICE

Which type of personal information should generally be kept private when using online services?

- ☐ **A** Your favorite color
- ☒ **B** Your full government-issued identification number
- ☐ **C** Your opinion about a public news article
- ☐ **D** Your preferred operating system

ANSWER B

WHY Government-issued identification numbers (such as a Social Security Number or national ID) are highly sensitive personal data that can be used for identity theft if exposed. Favorite colors, public opinions, and operating system preferences are not sensitive personally identifiable information.

QUESTION 5

SINGLE CHOICE

Which of the following is the BEST description of netiquette?

- ☐ A A technical standard for routing packets across the Internet
- ☒ B A set of accepted rules and conventions for polite and respectful online behavior
- ☐ C A type of license that governs the reuse of online content
- ☐ D A protocol used by email servers to transfer messages

ANSWER B

WHY Netiquette refers to the customary code of polite behavior on the Internet, including respecting others' opinions, avoiding all-caps (which implies shouting), and using clear, respectful language. The other options describe unrelated technical concepts: routing, licensing, and email transport.

QUESTION 6

SINGLE CHOICE

In an email message, what is the primary purpose of the Subject line?

- ☐ A To authenticate the sender's identity to the receiving mail server
- ☐ B To encrypt the message contents during transit
- ☒ C To provide a brief preview of the message topic for the recipient
- ☐ D To attach large files to the message

ANSWER C

WHY The Subject line is intended to summarize the topic of the email so recipients can quickly understand its purpose before opening it. Authentication, encryption, and attachment handling are functions of other email mechanisms, not the Subject field.

QUESTION 7

MULTIPLE CHOICE

Which of the following are common warning signs that an email may be a phishing attempt? (Choose two.)

- ☒ **A** Urgent language demanding immediate action, such as verifying an account within 24 hours
- ☐ **B** A message that comes from a coworker you regularly correspond with on the same topic
- ☒ **C** Generic greetings like 'Dear Customer' rather than your real name
- ☐ **D** A signature block that includes the sender's full name and company contact information

ANSWER A • C

WHY Phishing emails commonly use urgency to pressure victims and address them generically because attackers send bulk messages without personal details. A familiar coworker on a normal topic and a complete, legitimate signature block are not typical indicators of phishing.

QUESTION 8

SINGLE CHOICE

Which term describes software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system?

- ☐ **A** Utility software
- ☒ **B** Malware
- ☐ **C** Open-source software
- ☐ **D** Firmware

ANSWER B

WHY Malware is the umbrella term for malicious software such as viruses, worms, trojans, ransomware, and spyware that are designed to harm systems or steal data. Utility software performs helpful tasks, open-source software refers to a licensing model, and firmware is low-level software embedded in hardware.

QUESTION 9

SINGLE CHOICE

A user wants to participate in an online discussion forum where messages are organized into threads by topic. Which type of online communication tool is the user MOST likely using?

- ☐ A An email client
- ☒ B A discussion forum or message board
- ☐ C A peer-to-peer file-sharing network
- ☐ D A video conferencing platform

ANSWER B

WHY Discussion forums and message boards organize user posts into threads by topic, allowing asynchronous conversations. Email is generally one-to-one or one-to-many but not threaded by topic in the same structured way, and the other options serve different purposes.