Name: _____ **Date:** _____

Answer Key: Cybersecurity Logic Challenge for 4th Grade

Risk assessment, digital footprint analysis, and multi-factor authentication concepts. This advanced evaluation reinforces defensive thinking and proactive digital citizenship.

---

1. An online game platform asks you to download a 'Super-Speed Patch' from a third-party website to make your character run faster. What is the most logical first step to analyze this situation?

Answer: B) Check if the official game developer released the patch.

Evaluating the source is a critical cybersecurity skill. Genuine updates come from the original creator, while third-party 'patches' are frequent delivery methods for malware.

2. A digital footprint only includes things you intentionally post, like photos or comments, and does not include websites you visit or things people tag you in.

Answer: B) False

A digital footprint is a cumulative record of your online activity, including passive data collection and information shared by others about you.

3. A hacker uses a program to quickly try thousands of common words to guess a password. This is called a 'Brute Force' attack. Which password would be the hardest for this program to crack?

Answer: C) Tr0p!c#Kiw19

Complexity—using a mix of uppercase, lowercase, numbers, and special symbols—increases the time and computing power required for a hacker to guess a password.

4. While using a school computer, you find that the student who used it before you forgot to log out of their email. What is the most responsible action to take?

Answer: C) Log them out immediately without looking at their data.

Ethical cybersecurity behavior involves respecting the privacy of others. Logging them out protects their data without overstepping boundaries.

5. Two-Factor Authentication (2FA) is safer than just a password because a hacker would need both your password and your physical device to get into your account.

Answer: A) True

Name: _____ **Date:** _____

2FA adds a layer of 'something you know' (password) and 'something you have' (phone/token), making unauthorized access much more difficult.

6. You receive a text message saying 'Your tablet has a virus! Click here to clean it.' This is an example of 'Smishing.' What is the primary goal of the sender?

Answer: B) To trick you into giving away personal info or clicking a link.

Smishing (SMS Phishing) uses high-pressure language or fear to manipulate users into taking an unsafe action, like clicking a malicious link.

7. You are creating a profile for a new educational app. Which set of information is the SAFEST to share publicly?

Answer: B) A creative avatar, a nickname, and your favorite color.

Minimizing Personally Identifiable Information (PII) reduces the risk of identity theft or social engineering attacks.

8. If a website has a padlock icon in the address bar (HTTPS), it means the website is 100% safe and the people running it can be trusted with your secrets.

Answer: B) False

The padlock means the connection is encrypted (private), but it does not guarantee the website's owners are honest. Scammers can also use HTTPS.

9. A 'Firewall' is a security system that monitors incoming and outgoing network traffic. Which of the following best describes its job?

Answer: B) A filter that blocks unauthorized data from entering a network.

A firewall acts as a gatekeeper, inspecting data packets and blocking those that do not meet specific security criteria.

10. While gaming, another player offers to give you 'free currency' if you give them your login token or cookie info. Why is this a major security risk?

Answer: B) Tokens can allow them to bypass your password and take your account.

Session tokens and cookies are digital 'keys' that tell a website you are already logged in. Sharing them is like giving away a key to your house.