Name: _____ **Date:** _____

Answer Key: Cybersecurity Fundamentals Quiz for 11th Grade

How do digital certificates and SQL injections impact your safety? Identify core defense mechanisms in this 10-question assessment.

---

1. A student receives an email that appears to be from their university's IT department asking them to 're-verify' their credentials via a link. This is an example of which social engineering tactic?

Answer: B) Spear Phishing

Spear phishing is a targeted attempt to steal sensitive information such as account credentials by masquerading as a trusted entity in an electronic communication.

2. Biometric authentication, such as facial recognition or fingerprint scanning, is considered more secure than a standard password because it is unique to the individual.

Answer: A) True

Biometrics provide an additional layer of security based on intrinsic physical traits that are much harder for hackers to 'guess' or steal than text-based passwords.

3. When browsing the web, the presence of 'HTTPS' in the URL bar indicates that the data transmitted between your browser and the server is _____.

Answer: C) Encrypted

HTTPS uses SSL/TLS protocols to encrypt data, ensuring that sensitive information like credit card numbers cannot be read by eavesdroppers during transmission.

4. Which of the following describes 'Zero Day' vulnerability?

Answer: B) A software flaw unknown to the developer that is exploited by hackers

A Zero Day vulnerability is a security hole in software that is unknown to the vendor, meaning the developer has 'zero days' to fix it before it can be exploited.

5. Using the same password across multiple high-stakes accounts (like banking and personal email) is a safe practice as long as the password is long.

Answer: B) False

Name: _____ **Date:** _____

Password reuse is a major security risk; if one site suffers a data breach, hackers can use those credentials to access all other accounts using that same password.

6. A specialized piece of software or hardware that monitors and filters incoming and outgoing network traffic based on security rules is called a _____.

Answer: C) Firewall

Firewalls act as a barrier between a trusted network and an untrusted network (like the internet), blocking malicious traffic based on pre-defined security criteria.

7. What is the primary purpose of a Virtual Private Network (VPN) when using a public Wi-Fi network at a coffee shop?

Answer: C) To create a secure, encrypted tunnel for your data traffic

VPNs encrypt your internet connection, making it difficult for others on the same public network to intercept or view your sensitive activities.

8. The security practice of requiring two or more pieces of evidence to verify a user's identity is known as _____ Authentication.

Answer: C) Multi-Factor

Multi-Factor Authentication (MFA) requires users to provide two or more verification factors (like a password and a phone code) to gain access to a resource.

9. 'Shoulder Surfing' refers to a physical security threat where someone watches you enter your PIN or password over your shoulder.

Answer: A) True

Shoulder surfing is a form of social engineering where an attacker uses direct observation techniques to obtain sensitive information without the victim's knowledge.

10. Which of these is the most effective way to protect your smartphone from unauthorized access if it is stolen?

Answer: B) Enabling a remote wipe feature and using a strong passcode

Remote wipe allows you to erase all personal data from a distance, and a strong passcode prevents initial access to the device's functions.