Name: _______________ **Date:** _______________

Answer Key: Digital Firewall: A Cybersecurity Blueprint for College Freshmen

How do hackers exploit human psychology? This mixed-format quiz identifies fundamental security protocols and threat vectors in professional digital environments.

1. In the context of organizational security, what is the primary purpose of an 'Air Gap'?

Answer: B) To physically isolate a secure network from unsecured networks like the public internet

An air gap is a security measure that ensures a computer or network is physically isolated from unsecured networks, making remote hacking virtually impossible.

2. Biometric authentication, such as fingerprint or facial recognition, is considered a 'something you are' factor in multi-factor authentication.

Answer: A) True

Authentication factors are categorized as something you know (password), something you have (token), or something you are (biometrics).

3. Which of the following describes 'vishing' in a professional setting?

Answer: B) A phishing attack conducted over phone calls or voice messages

Vishing, or 'voice phishing', involves using telephony to trick individuals into revealing sensitive financial or personal information.

4. A university student receives an email claiming to be from the 'IT Help Desk' asking them to click a link to 'validate their mailbox quota.' This is an example of:

Answer: A) Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

5. Using a Virtual Private Network (VPN) on a public Wi-Fi network creates an encrypted 'tunnel' for your data, making it harder for others on the same network to intercept your traffic.

Answer: A) True

Name: ________________ **Date:** ________________

VPNs encrypt data packets at the source and decrypt them at the destination, protecting information from 'packet sniffing' on open networks.

6. Which of these is the most secure method for managing multiple complex passwords across different academic and personal accounts?

Answer: C) Utilizing a dedicated password manager with a single, unique master password

Password managers allow users to use unique, highly complex passwords for every site while only needing to remember one master key.

7. In cybersecurity, the 'principle of least privilege' (PoLP) suggests that users should be given:

Answer: B) Only the minimum levels of access necessary to perform their job functions

PoLP limits the potential damage of a compromised account by ensuring no user has more access than they absolutely require.

8. Software updates and 'patches' are primarily released to add new aesthetic features and rarely contain security fixes.

Answer: B) False

Patches are critical because they often fix 'vulnerabilities'—flaws in the code that hackers use to gain unauthorized access.

9. What is the primary risk of 'tailgating' in the context of physical security at a data center or office?

Answer: A) An unauthorized person following an authorized person into a restricted area

Tailgating is a physical social engineering technique where an attacker gains entry to a secure facility by following someone with legitimate access.

10. If you suspect your college email account has been compromised, your first instructional step should be to:

Answer: C) Report the incident to IT and change your password from a known clean device

Immediate reporting and password rotation from a secure device are standard incident response steps to mitigate further unauthorized access.