Name: _____ **Date:** _____

Answer Key: Hack-Proof Your Habits: 6th Grade Cyber Strategy Quiz

Evaluate digital defense methods by analyzing polymorphic malware threats and the efficacy of zero-trust verification protocols in modern networking.

---

1. An attacker uses a 'Man-in-the-Middle' (MitM) attack to intercept data on an unencrypted public Wi-Fi network. Which technology would have been the most effective preventative measure for the user?

Answer: B) A Virtual Private Network (VPN) tunnel

A VPN creates an encrypted tunnel for data, making it unreadable to attackers even if they manage to intercept the transmission on a public network.

2. When an individual receives a highly personalized email that uses their real name and mentions a recent specific purchase to trick them into clicking a malicious link, this targeted attack is known as _____.

Answer: C) Spear Phishing

Spear phishing is a specialized form of phishing that targets a specific individual or group by using personal details to build false trust.

3. Biometric authentication, such as facial recognition or fingerprint scanning, 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), and something you are (biometrics).

4. Consider the 'Internet of Things' (IoT). Why does a smart refrigerator or a web-connected thermostat often pose a significant cybersecurity risk to a home network?

Answer: B) They often lack robust security updates and use default passwords

Many IoT devices are manufactured with 'hardcoded' or default passwords and rarely receive security patches, making them easy entry points for hackers.

5. If a hacker locks a local library's database and demands a payment in cryptocurrency to provide the decryption key, the library is a victim of a _____ attack.

Name: _____ **Date:** _____

Answer: C) Ransomware

Ransomware is malware designed to deny access to a computer system or data until a sum of money is paid.

6. Using the same strong, complex password across multiple banking and social media accounts is an effective way to maintain high security.

Answer: B) False

Reusing passwords creates a single point of failure; if one site suffers a data breach, all other accounts using that password become vulnerable to 'credential stuffing' attacks.

7. Which of these is the most sophisticated way to verify if a website is authentic and uses HTTPS encryption?

Answer: C) Inspecting the site's SSL/TLS certificate details in the browser

SSL/TLS certificates are issued by trusted authorities to verify the identity of the website owner and ensure the connection is encrypted.

8. The security principle of _____ suggests that a user should only be given the minimum levels of access – or permissions – needed to perform their job.

Answer: B) Least Privilege

The 'Principle of Least Privilege' limits the potential damage from an accident or a compromised account by restricting access to only what is necessary.

9. Software 'patches' and updates are primarily released to add new cosmetic features, and ignoring them does not impact the security of the device.

Answer: B) False

Updates often contain critical 'security patches' that fix vulnerabilities hackers use to gain unauthorized access to systems.

10. In the context of incident response, why is it critical to 'isolate' a device from the network immediately after discovering a malware infection?

Answer: A) To prevent the malware from spreading to other connected devices

Isolation prevents 'lateral movement,' where a virus or worm uses the local network to infect other computers, servers, or smart devices.

Name: _____ Date: _____