Name: _____ **Date:** _____

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?

A. Incognito or Private browsing mode
B. A Virtual Private Network (VPN) tunnel
C. Clearing the browser cache regularly
D. Increasing the screen brightness

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 _____.

A. General Phishing
B. Smishing
C. Spear Phishing
D. Vishing

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

A. True
B. False

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?

A. They use too much electricity, causing firewalls to fail
B. They often lack robust security updates and use default passwords
C. They convert digital signals into analog waves that bypass routers
D. They are too small to contain encryption software

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.

A. Adware
B. Spyware
C. Ransomware
D. Trojan Horse

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

Name: _____ Date: _____

A. True
B. False

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

A. Checking if the website looks professional and has no typos
B. Clicking the 'About Us' page to see if there is a phone number
C. Inspecting the site's SSL/TLS certificate details in the browser
D. Searching for the website on a social media platform

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.

A. Maximum Redundancy
B. Least Privilege
C. Open Access
D. Social Engineering

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

A. True
B. False

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

A. To prevent the malware from spreading to other connected devices
B. To allow the battery to charge faster for the cleanup
C. Because malware cannot live on a device that isn't online
D. To notify the internet service provider automatically