Name: _____ **Date:** _____

Answer Key: Invisible Shields: A 9th Grade Cybersecurity Awareness Quiz

Digital hygiene, social engineering, and metadata safety—essential behaviors for securing your virtual identity in an increasingly connected world.

---

1. When connecting to a public Wi-Fi network at a local cafe, which technology acts as a secure tunnel to prevent others on the network from snooping on your data?

Answer: A) A Virtual Private Network (VPN)

A VPN encrypts your internet traffic and routes it through a secure server, making it unreadable to hackers who might be monitoring public Wi-Fi traffic.

2. Using the same strong password across multiple social media platforms is considered a safe cybersecurity practice as long as the password contains symbols and numbers.

Answer: B) False

This practice is dangerous because if one site suffers a data breach, hackers can 'credential stuff' or use those credentials to gain access to all your other accounts.

3. The process of verifying your identity using two different methods—such as a password plus a fingerprint or a code sent to your phone—is known as _____.

Answer: C) Multi-Factor Authentication (MFA)

MFA (or 2FA) adds a critical layer of security by requiring more than just a password to access an account.

4. You receive an urgent DM from a 'Moderator' stating your account will be deleted in 1 hour unless you click a link to verify your ID. This is an example of:

Answer: B) A social engineering attack

Social engineering uses psychological manipulation, such as creating a false sense of urgency, to trick people into divulging sensitive information.

5. Photos posted online often contain 'EXIF data' which can reveal the exact GPS coordinates of where the photo was taken.

Answer: A) True

Name: _____ **Date:** _____

Metadata stored within image files can include location, time, and device information, which is why many privacy experts recommend stripping EXIF data before sharing photos.

6. Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system is collectively referred to as _____.

Answer: D) Malware

Malware is a broad term that includes viruses, worms, trojans, and ransomware designed to harm or exploit systems.

7. Which of these is the most secure way to manage dozens of unique, complex passwords for various school and personal accounts?

Answer: C) Using an encrypted password manager

Password managers encrypt your login data and can generate high-entropy passwords that are nearly impossible to guess.

8. If your social media account is hacked, the first thing you should do after regaining access is to notify your followers so they don't click on any malicious links sent from your account.

Answer: A) True

Part of incident response is damage mitigation; letting others know helps prevent the 'infection' from spreading to your friends and family.

9. The padlock icon in your browser's address bar indicates that the website is using _____, which encrypts the data sent between your computer and the server.

Answer: B) HTTPS

HTTPS (Hypertext Transfer Protocol Secure) ensures that communication is encrypted using TLS/SSL certificates.

10. Why is it important to keep your computer's operating system (like Windows, macOS, or ChromeOS) updated to the latest version?

Answer: C) To receive security patches that fix known vulnerabilities

Developers release updates to 'patch' or close security holes that hackers have discovered and might otherwise use to enter your system.