Name: _____ **Date:** _____

Answer Key: Shatter the Screen: Can You Outsmart the 8th Grade Cyber-Sentinels?

Gain the upper hand against invisible threats by analyzing social engineering tactics and mastering the mechanics of end-to-end encryption and digital footprints.

---

1. A hacker uses a technique called 'Whaling' to target a high-ranking executive. What is the primary characteristic of this specific attack?

Answer: B) A highly personalized phishing attack aimed at high-profile individuals

Whaling is a specialized form of phishing that targets high-level executives (the 'big fish') using sophisticated, personalized information to gain access to corporate secrets.

2. End-to-end encryption (E2EE) ensures that service providers like Apple or WhatsApp can decrypt and read your messages if required by law.

Answer: B) False

In true E2EE, only the sender and recipient hold the cryptographic keys; even the service provider hosting the message cannot view the plaintext content.

3. When a website uses HTTPS instead of HTTP, it means the communication between your browser and the server is secured using ___.

Answer: A) TLS (Transport Layer Security)

TLS (the successor to SSL) provides the encryption and authentication needed to turn standard web traffic into secure HTTPS traffic.

4. Which of these concepts refers to the trail of data you intentionally leave behind, such as social media posts and forum comments?

Answer: C) Active digital footprint

An active digital footprint is created when a user deliberately shares information about themselves, whereas a passive footprint is collected without the user's direct action.

5. Malware that locks a user's files and demands payment to restore access is known as ___.

Answer: C) Ransomware

Name: _____ **Date:** _____

Ransomware encrypts a victim's data and forces them to pay a fee (often in cryptocurrency) to receive the decryption key.

6. Biometric authentication, such as facial recognition, is considered a more secure 'factor' than a password alone because it is something you ARE, rather than something you KNOW.

Answer: A) True

Multifactor authentication (MFA) relies on three categories: something you know (password), something you have (phone), and something you are (biometrics).

7. You receive a message from a friend on Discord with a link to a 'free gift card.' The link looks like 'd1scord.gift/promo'. This is an example of what tactic?

Answer: A) Typosquatting

Typosquatting (or URL hijacking) involves registering domain names that are slightly misspelled versions of popular sites to trick users into visiting malicious pages.

8. The ethical practice where hackers are hired to find vulnerabilities in a system so they can be fixed is called ___ hacking.

Answer: B) White-hat

White-hat hackers use their skills for defensive purposes, often working as security consultants to improve a company's defenses.

9. Which of the following is the most secure way to handle a suspicious text message claiming your Amazon account has been compromised?

Answer: C) Delete the text and log into Amazon directly through a trusted browser

Navigating directly to the official website ensures you are on a legitimate platform, avoiding the potential phishing link in the text.

10. Using a Virtual Private Network (VPN) on public Wi-Fi makes your data invisible to the Wi-Fi owner, but it does NOT protect you from downloading malware manually.

Answer: A) True

A VPN creates a secure tunnel for data transmission, but it cannot stop a user from clicking a malicious download link within that secure tunnel.