

Name: _____ Date: _____

Answer Key: Glitch Trap: 5th Grade Cyber-Defense Intelligence Quiz

Armor up as an elite security analyst to dissect complex social engineering tactics and secure vulnerabilities in this high-stakes formative assessment.

1. An online gaming friend you've known for a week sends you a link to a 'Secret Mod' that requires you to disable your firewall to install it. What is the most likely risk?

Answer: B) A Trojan horse could bypass your security to steal local data.

Disabling a firewall removes the barrier between your device and malicious software; 'secret' files from unverified sources often contain Trojans designed to infiltrate systems.

2. Using the same complex password for your school login and your private social media account is an example of 'credential stuffing' protection.

Answer: B) False

Reusing passwords makes you vulnerable to credential stuffing, where a hacker uses a password leaked from one site to break into all your other accounts.

3. When an attacker calls you pretending to be IT support to trick you into giving up your password, they are using a social engineering tactic called _____.

Answer: B) Vishing

Vishing (voice phishing) is a specific type of social engineering where attackers use phone calls to manipulate people into revealing sensitive information.

4. You see an ad claiming your tablet is infected with 15 viruses and you must click 'Repair Now.' This is a common example of:

Answer: C) Scareware

Scareware uses false alarms to frighten users into downloading malware or paying for useless software.

5. In a 'Man-in-the-Middle' attack, a hacker may intercept data you send over an unsecured public Wi-Fi network at a coffee shop.

Answer: A) True

Name: _____ **Date:** _____

Unsecured networks allow attackers to sit 'between' you and the website you are visiting to capture your usernames, passwords, and messages.

6. Biometric authentication uses your physical traits for security. Which of these is a form of _____ authentication?

Answer: B) Fingerprint scanning

Biometrics identify users through unique physical characteristics like fingerprints, facial recognition, or iris patterns.

7. Why is it important to check the 'Privacy Policy' of a new app before clicking 'Accept'?

Answer: B) To verify if the app sells your location data to third parties

Privacy policies detail how a company collects, uses, and shares your personal information and data.

8. A 'Zero-Day' vulnerability is a security hole that the software creator has known about for exactly zero days, meaning no patch exists yet.

Answer: A) True

Zero-day threats are exploited by hackers before a fix is released, making them extremely dangerous.

9. To keep your tablet safe from the latest threats, you should always enable _____ updates for your apps and operating system.

Answer: C) Automatic

Automatic updates ensure that security patches are installed as soon as they are available, closing vulnerabilities quickly.

10. Which behavior is the best defense against 'Shoulder Surfing' in a public library?

Answer: B) Using a privacy screen filter or covering your hands while typing

Shoulder surfing is when someone watches you enter private info; physical barriers like privacy screens or your hands help prevent this.