Answer Key: Neon Shield: The 8th Grade Digital Defense Quest

Construct a solid foundation in network safety by identifying 10 key security concepts including biometric locks, firewall basics, and digital footprints.

---

1. Which of these is a form of biometric authentication often used to secure modern smartphones?

Answer: C) Facial recognition or fingerprint scanning

> Biometrics use unique physical characteristics, such as your face or fingerprint, to verify your identity.

2. True or False: Using the same password for your school email and your gaming account is a safe practice as long as the password is long.

Answer: B) False

> Password reuse is dangerous; if one account is breached, hackers can use those credentials to access all your other accounts.

3. A ____ is a digital barrier that monitors and controls incoming and outgoing network traffic based on security rules.

Answer: B) Firewall

> Firewalls act like security guards for a network, blocking unauthorized access while allowing safe data to pass through.

4. What should you do if you receive a 'Critical Alert' pop-up on a website claiming your computer has 50 viruses and providing a phone number to call?

Answer: C) Close the browser tab and do not call the number.

> These are 'scareware' tactics designed to trick you into calling scammers or downloading actual malware.

5. The permanent record of all the information you leave behind online, including comments and likes, is known as your digital ____.

Answer: B) Footprint

> A digital footprint represents the trail of data you create while using the internet, which can be seen by others.

---

6. True or False: If a website's URL begins with 'https://', it means the data sent between your browser and the site is encrypted.

Answer: A) True

> The 's' in https stands for 'secure' and indicates that the site uses SSL/TLS encryption for data transmission.

7. Which of these is the most secure way to handle a suspicious link sent to you by a 'friend' on social media whose account might be hacked?

Answer: B) Message the friend on a different app to verify they sent it.

> Verifying through a different communication channel (out-of-band) helps confirm if the sender's account was compromised.

8. When a person uses the internet or mobile phones to intentionally upset or intimidate someone else, it is called _____.

Answer: C) Cyberbullying

> Cyberbullying involves using digital platforms to harass or target individuals, which is a major concern for online safety.

9. True or False: Software updates for your computer or apps often include 'patches' that fix security vulnerabilities.

Answer: A) True

> Developers release updates to 'patch' or fix holes that hackers might use to enter your system.

10. Your friend suggests downloading a 'free' version of a popular paid game from an unofficial website. What is the primary cybersecurity risk?

Answer: B) The file could contain a Trojan horse or other malware.

> Unofficial or 'pirated' software is a common way for hackers to distribute malware disguised as something useful.