Score:

Reporter (R): Good morning, and welcome to "Tech Insight." Today I'm speaking with Dr. Elena Ruiz, a cybersecurity specialist. Dr. Ruiz, thanks for joining us.
Expert (E): Thank you for having me.
R: Let's begin: Do you think **social media** platforms are more of a benefit or a risk in the era of **digitalization**?
E: That's a great question. In my view, social media play a crucial role in connecting people globally, but they also pose serious challenges in **privacy** and **cybersecurity**.
R: Some critics argue that platforms harvest personal data without proper **encryption** or consent. What's your take?
E: Indeed, platforms often collect vast amounts of **data analytics**, which may be vulnerable — **malware**, **phishing** attacks, and **data breaches** are real dangers.
R: So would you say that encryption is a safeguard or just a partial solution?
E: Encryption is essential, but it's not foolproof. Hackers can exploit system vulnerabilities. Also, because of **automation** and AI, attacks evolve rapidly.
R: One more question: Do you think that going "off-network" or even **digital detox** is advisable for users concerned about privacy?
E: Maybe. Sometimes a digital detox is helpful to reset one's habits. But realistically, as everything becomes connected via **IoT**, going fully offline is unlikely.
R: In summary, what do you see as the major future shift in social networks?
E: I believe we'll see increased integration with augmented reality, virtual reality, and more AI-driven customization, but only if robust cybersecurity measures and privacy safeguards are adopted by design.
R: You mentioned AI integration. Do you think regulation is keeping pace with innovation?
E: Not really. In fact, there's often a lag — new features are rolled out before legislation can adapt. And that gap can be exploited by malicious actors.
R: So, would you say users are left vulnerable during that period?
E: Absolutely. Even with regulation, platforms may find ways to bypass rules or delay compliance. Meanwhile, data is still being collected — sometimes without clear consent.
R: Some claim that apps mislead users about how secure they really are. Is that true?
E: Unfortunately, yes. Some apps are promoted as secure but are later revealed to have backdoors or flawed encryption.
R: If that's the case, what options do users have?
E: Well, they can try to adjust privacy settings or reduce usage, but realistically, you can't simply opt out — the ecosystem is too interconnected.
R: Final thoughts?
E: Regulation must evolve as quickly as the technology does. Otherwise, we'll always be reacting instead of preventing threats.

1. _____ It can be inferred that social media platforms are considered useful for global communication, even though they involve privacy risks.
2. _____ It can be inferred that Dr. Ruiz believes encryption completely eliminates all cybersecurity threats.
3. _____ It can be inferred that cyberattacks are becoming more sophisticated due to the use of AI and automation.
4. _____ It can be inferred that users always have full control over how their personal data is collected and used.
5. _____ It can be inferred that a digital detox may help users temporarily reduce their dependence on technology.
6. _____ It can be inferred that completely disconnecting from the internet is considered a realistic long-term solution for most users.
7. _____ It can be inferred that there is often a delay between technological innovation and legal regulation.
8. _____ It can be inferred that all mobile applications are fully transparent about their security features.
9. _____ It can be inferred that users are sometimes vulnerable because data may still be collected even when regulations exist.
10. _____ It can be inferred that improving cybersecurity requires both technological updates and stronger legal frameworks.

LIVEWORKSHEETS