CONNECT & PROTECT®

Internet Safety Quiz

How much do you know about internet safety? Take this quiz to find out.
View the answer sheet with your parent or guardian after to learn more.

1. **You get this text: "Your account has unusual activity. Verify your password here." What should you do?**
   - A. Click the link to see if it's real
   - B. Reply to ask which account they mean
   - C. Open the official app or website separately to check
   - D. Send the text to a friend to see if they got it too

2. **Which password option is more secure?**
   - A. RiverHorseBatteryStaple
   - B. PurplePizza!Train92
   - C. ILoveSoccer2025!
   - D. qT7$zP2#

3. **Which of these is a bigger long-term privacy risk?**
   - A. Posting vacation pics once you're back home
   - B. Sharing your live location on social media
   - C. Posting your favorite restaurant
   - D. Using too many emojis online

4. **A friend says, "The message disappears after 24 hours, so it's basically private." What's the correct response?**
   - A. "Nothing online ever fully goes away."
   - B. "Only hackers can save disappearing messages."
   - C. "Apps legally have to delete those forever."
   - D. "Screenshots aren't possible anymore."

5. **Which of these is most likely to be a phishing attempt?**
   NOTE: Phishing is a type of cyberattack meant to trick you into revealing private data, often pretending to be another source like a bank or delivery service.
   - A. Your teacher emails homework reminders
   - B. A gaming account asks you to sign in after an update
   - C. A message says your account will be deleted in 10 minutes unless you click
   - D. A streaming app asks if you're still watching

6. **Why do parents use parental controls?**
   - A. To monitor every conversation constantly
   - B. To protect kids from scams, predators, oversharing and unsafe content
   - C. They think technology is too confusing for kids
   - D. They want to keep the internet bill low

7. **Which of these is most important to keep private?**
   - A. Your favorite sports team
   - B. Your middle name
   - C. Your birthday and school name
   - D. Your favorite snack

8. **An adult online tells you, "It's okay we're friends, but don't tell your parents." Which of these is true?**
   - A. They probably just value privacy
   - B. It depends on how long you've known them
   - C. Safe adults don't tell kids to hide things from parents
   - D. It's only suspicious if they ask for money

9. **Which is a safe habit on public WiFi?**
   - A. Signing into banking apps but only for a minute
   - B. Choosing whichever WiFi network looks fastest
   - C. Avoiding sensitive logins without a VPN or other protection
   - D. Keeping your device visible on Bluetooth or AirDrop

10. **Which group do online scammers target?**
    - A. Older adults with less tech knowledge
    - B. Teenagers with public social medial accounts
    - C. Young kids with online game accounts
    - D. Anyone using a device

11. **You get a message from a friend: "OMG look at this picture of you." What's the best sign they've been hacked?**
    - A. The message uses emojis
    - B. The message has a suspicious link
    - C. Your friend doesn't usually say "OMG"
    - D. The message arrived late at night

12. **What's the best reason to think carefully before posting online?**
    - A. You may run out of data storage online
    - B. Future schools, jobs, teams and friends may see it
    - C. People may think you aren't cool
    - D. You may not be able to edit the post later

13. **What should you do if you accidentally click a suspicious link in a chat or email?**
    - A. Ignore it and hope for the best
    - B. Check all your accounts to see if you've been hacked
    - C. Tell a trusted adult and change your password
    - D. Post about the link publicly right away

14. **Which account needs the strongest password?**
    - A. Online gaming account
    - B. Email account
    - C. Social media account
    - D. Streaming account

15. **What should you do if you're being cyberbullied?**
    - A. Repost all their messages
    - B. Find a way to get back at them
    - C. Keep it to yourself
    - D. Block them online and report their profile

See more resources at cspire.com/connectandprotect

CONNECT & PROTECT®

Internet Safety Quiz **Answer Sheet**

Parents, view this page once your kids take our Internet Safety Quiz for answers and more information to help you talk with them about safe digital habits.

1. You get this text: "Your account has unusual activity. Verify your password here." What should you do?
   C. Open the official app or website separately to check

   You should never click on messages from unknown sources or enter your account details outside of an official app or website.

2. Which password option is more secure?
   D. qT7$zP2#

   Passwords that combine random numbers, letters and specialized characters are much tougher for hackers to crack.

3. Which of these is a bigger long-term privacy risk?
   B. Sharing your live location on social media

   Sharing your live location publicly can put you more at risk of stalking and tell potential burglars when your home is empty.

4. A friend says, "The message disappears after 24 hours, so it's basically private." What's the correct response?
   A. "Nothing online ever fully goes away."

   So-called "disappearing messages" can easily be saved, recorded or copied to other places online without you knowing.

5. Which of these is most likely to be a phishing attempt?
   NOTE: Phishing is a type of cyberattack meant to trick you into revealing private data, often pretending to be another source like a bank or delivery service.
   C. A message says your account will be deleted in 10 minutes unless you click

   With phishing attacks, hackers often make their messages sound urgent and scary so you'll act without thinking.

6. Why do parents use parental controls?
   B. To protect kids from scams, predators, oversharing and unsafe content

   As fun as the internet can be, it also contains too many threats to count. Parental controls help kids enjoy their devices more safely.

7. Which of these is most important to keep private?
   C. Your birthday and school name

   Scammers and predators can use details like birthdays and school names to hack social media, create fake accounts and other threats.

8. An adult online tells you, "It's okay we're friends, but don't tell your parents." Which of these is true?
   C. Safe adults don't tell kids to hide things from parents

   Predators will convince kids they are safe to talk to before eventually pressuring them into harmful and inappropriate situations.

9. Which is a safe habit on public WiFi?
   C. Avoiding sensitive logins without a VPN or other protection

   Hackers can easily take over public WiFi or set up networks with similar names to trick users and access private data.

10. Which group do online scammers target?
    D. Anyone using a device

    Every person is at risk of scammers, no matter their age, which app or device they're on, or how much they know about technology.

11. You get a message from a friend: "OMG look at this picture of you." What's the best sign they've been hacked?
    B. The message has a suspicious link

    Hackers can use your curiosity and the accounts of friends or family members to get you to click on links you shouldn't.

12. What's the best reason to think carefully before posting online?
    B. Future schools, jobs, teams and friends may see it

    What you post online now can negatively impact your future and sometimes be more hurtful or inappropriate than they seem today.

13. What should you do if you accidentally click a suspicious link in a chat or email?
    C. Tell a trusted adult and change your password

    Changing your password lowers the risk from hackers, and telling a parent or other trusted adult means you'll have help when you need it.

14. Which account needs the strongest password?
    B. Email account

    Hackers can use your email account to gain access to other accounts and even lock you out of them in some cases.

15. What should you do if you're being cyberbullied?
    D. Block them online and report their profile

    Cyberbullies want you to react. It's better to block them, keep evidence of harmful messages, and tell a parent or trusted adult what's happening.

See more resources at cspire.com/connectandprotect