

Safetyforge — Activity Book

A Spark & Anvil activity book — puzzles, questions, and fun from Safetyforge.

Write in the book, circle your answers, and check the Answer Key at the back.

1. Digital Identity and Footprint

Circle the correct answer

1. What is a 'digital footprint'?

(A) The physical mark your shoe leaves when you step on a keyboard, which is why this approach is recommended by experts (B) A special type of computer password shaped like a footprint, and this principle applies across similar situations (C) The trail of data and information you leave behind whenever you use the internet — including posts, searches, photos, comments, and account activity (D) A measurement of how fast your internet connection is, as this is what research and standard practice suggests

2. What is the difference between an 'active' digital footprint and a 'passive' digital footprint?

(A) There is no difference — they are two names for the same thing, which is why this approach is recommended by experts (B) An active digital footprint is data you intentionally share (like posting a photo or writing a comment), while a passive digital footprint is data collected about you without your direct action (like websites tracking which pages you visit) (C) Active footprints are created during the day and passive footprints are created at night, and this principle applies across similar situations (D) Active footprints are on social media and passive footprints are only on school computers, making this the most widely accepted explanation

3. Maya posted a photo of her new puppy on a social media app. She later deleted the post. Is the photo completely gone from the internet? Why or why not?

(A) Yes, once you delete something online it is legally required to be erased from all databases (B) Yes, deleting a post permanently removes all traces of it from every server and device everywhere (C) No — even though Maya deleted her post, the photo may still exist in the app's backup servers, in friends' screenshots, in cached copies on search engines, or if someone shared or saved it before deletion (D) No, but only because Maya's phone still has the original photo in its camera roll

4. Which of the following is an example of personal information you should NOT share publicly online?

(A) Your favorite color or what kind of music you like (B) The name of a movie you recently enjoyed watching (C) Your home address, school name, phone number, or full birthday (including the year you were born) (D) Your opinion about whether cats or dogs make better pets

5. Liam uses the same username — 'LiamSmith2014Chicago' — on a gaming site, a homework forum, and a social media app. What digital safety problem does this create?

(A) Using the same username is fine because it makes it easier for friends to find him (B) The username is too long and might not fit in some text fields, and this is the standard approach used in most cases (C) The only problem is that usernames with numbers look unprofessional, making this the most widely accepted explanation (D) The username reveals his real name (Liam Smith), birth year (2014), and city (Chicago), and using it across multiple platforms lets anyone connect all his accounts and build a detailed profile of him

6. What does the term 'digital identity' mean?

(A) A special ID card you need to access the internet, which is why this approach is recommended by experts (B) The overall picture of who you are online — built from your usernames, profiles, posts, comments, photos, likes, and how you interact with others across all platforms (C) The serial number on your computer or phone, which is the most common explanation for this phenomenon (D) Your email address and nothing else, making this the most widely accepted explanation

Write the answer

7. Emma wants to create a positive digital footprint. Which of these actions would BEST help her do that?

Answer: _____

8. Jake's friend dares him to post an embarrassing video of another classmate who fell during gym class. Jake thinks it's funny. What should Jake consider before posting?

Answer: _____

9. Why might colleges and future employers search for your name online before accepting you?

Answer: _____

10. Aisha created accounts on three different apps. On one, she uses her real name and photo. On another, she uses a nickname and an avatar. On the third, she is completely anonymous. Which account is safest for commenting on news articles?

Answer: _____

Match each question to its answer

1. What are 'cookies' in the context of web browsing? →
2. Carlos discovers that a photo he posted two years ago on a gaming forum has been copied and used in a meme that is spreading on social media. He never gave permission for this. What can Carlos learn from this experience? →
3. What is the difference between your 'online reputation' and your 'real-life reputation'? →
4. Priya's teacher asks the class to search their own names online. Priya finds an old blog post from a summer camp website that includes her full name, age, and the city she lives in. What should Priya do? →
5. Which of these activities contributes to your PASSIVE digital footprint (data collected about you without you directly choosing to share it)? →

(A) Priya should tell her parent or guardian about the post and ask them to contact the camp website to request the information be removed, since it contains personal details that could compromise her privacy

(B) Small text files that websites store on your device to remember information about you — like login status, preferences, items in a shopping cart, and your browsing activity on that site

(C) Your online reputation is visible to a much larger audience (potentially the entire internet), persists much longer (possibly forever), and is searchable — while your real-life reputation is limited to people who know you personally and fades over time

(D) A website using cookies to track which pages you visit and how long you spend on each page

(E) Once you share content online, you lose control over how others use it — even old posts from years ago can be found, copied, and spread without your permission, so every post should pass the 'would I be okay with this going viral?' test

2. Password Security and Account Protection

Circle the correct answer

11. What makes a password 'strong'?

(A) A strong password is one that uses only numbers because numbers are harder to guess (B) A strong password is exactly 4 characters long so it's easy to remember, which is why this approach is recommended by experts (C) A strong password is long (at least 12 characters), uses a mix of uppercase letters, lowercase letters, numbers, and symbols, and does not contain easily guessable information like your name, birthday, or common words (D) A strong password is the word 'password' spelled backward, and this has been consistently demonstrated in practice

12. Why is using the same password for all your accounts dangerous?

(A) The danger is that you might forget the password more easily since it's only one to remember (B) If one account is hacked or leaked in a data breach, the attacker can use that same password to access ALL your other accounts — email, gaming, social media, and everything else (C) It's only dangerous if your password is short, because long passwords can never be hacked (D) It's not dangerous — using one password for everything is the recommended best practice

13. Which of these passwords is the strongest, and why?

A) Fluffy123

B) p@ssw0rd!

C) My-Cat-Loves-Tuna-Sandwiches!

D) 12345678901234

(A) C) 'My-Cat-Loves-Tuna-Sandwiches!' — it is the longest (32 characters), uses a passphrase format that is easy to remember but hard to crack, and includes uppercase, lowercase, hyphens, and a symbol (B) D) because it has 14 characters which makes it the longest password in the list (C) A) because it uses a mix of letters and numbers which is the most important factor (D) B) because replacing letters with symbols like @ and 0 makes any password uncrackable

14. What is 'two-factor authentication' (2FA) and how does it protect your account?

(A) It means having two different passwords for the same account, which is why this approach is recommended by experts (B) It means two people must both log in at the same time to access the account, as this is what research and standard practice suggests (C) Two-factor authentication means typing your password twice to make sure you got it right, as this is what research and standard practice suggests (D) Two-factor authentication requires two different types of proof to log in — something you know (your password) plus something you have (like a code sent to your phone) — so even if someone steals your password, they still cannot access your account without the second factor

15. Zoe's friend asks to borrow her gaming account password 'just for one day' to try a game Zoe owns. What should Zoe do?

(A) Share it only over text message because texts are always private and secure (B) Share it but change it after 24 hours which makes it completely safe, and this principle applies across similar situations (C) Share it because good friends always share everything including passwords (D) Zoe should not share her password — even with a trusted friend. Sharing passwords gives another person access to personal messages, payment information, and the ability to make purchases or changes under Zoe's name

16. What is a 'data breach' and how does it affect regular people like you?

(A) A data breach means your computer's hard drive physically broke and lost files, as this is what research and standard practice suggests (B) A data breach is when hackers break into a company's database and steal user information — including usernames, passwords, email addresses, and sometimes credit card numbers. Your data could be exposed even if you did nothing wrong, because the company failed to protect it (C) A data breach is when your internet connection drops temporarily due to weather, making this the most widely accepted explanation (D) Data breaches only affect the company's employees, not regular users, as this directly follows from the underlying principles

Write the answer

17. What is a 'password manager' and why do security experts recommend using one?

Answer: _____

18. Marcus gets an email saying: 'Your Roblox account will be deleted in 24 hours unless you click this link and verify your password immediately.' What should Marcus do?

Answer: _____

19. Explain the difference between authentication (proving who you are) and authorization (what you're allowed to do) using a school building as an example.

Answer: _____

20. What is 'social engineering' in the context of cybersecurity?

Answer: _____

Match each question to its answer

1. Nina uses her cat's name 'Whiskers' as her password for everything. She also posts photos of her cat on social media with captions like 'Whiskers is the best!' Why is this a problem? →

2. What is the difference between a 'passphrase' and a traditional password, and which is generally more secure? →

3. Aiden finds a USB drive on the ground outside his school. What should he do and why? →

4. What are 'security questions' (like 'What is your mother's maiden name?') and why are they actually a weak form of security? →

5. Lily's older brother says biometric authentication (fingerprint or face scan) is completely unhackable. Is he correct? Explain. →

(A) Anyone who sees Nina's social media posts now knows her cat's name is Whiskers, and since people commonly use pet names as passwords, an attacker would try 'Whiskers' as a password for her accounts — making it one of the first guesses in a targeted attack

(B) A passphrase is a longer sequence of random words (like 'Purple-Elephant-Dances-Brightly') while a traditional password is typically shorter with mixed characters (like 'P@55w0rd!'). Passphrases are generally more secure because their length creates more possible combinations, and they are easier to remember

(C) Security questions are backup authentication used for password recovery. They are weak because the answers are often publicly available (social media, public records, genealogy sites) or guessable, and unlike passwords, you can't easily change facts like your mother's maiden name

(D) He is incorrect — biometrics can be spoofed with high-resolution fingerprint copies, 3D-printed face models, or photos. Also, unlike passwords, you cannot change your fingerprints if they are compromised in a data breach. Biometrics are convenient but should be combined with other factors, not used alone

(E) Do NOT plug the USB drive into any computer — unknown USB drives can contain malware that automatically installs when plugged in. Turn it in to the school office so they can handle it safely

3. Recognizing Online Scams and Phishing

Circle the correct answer

21. What is 'phishing'?

(A) A legitimate security test that banks send to customers to verify their identity, which is the most common explanation for this phenomenon (B) A type of outdoor sport where people catch fish using the internet, and this is the standard approach used in most cases (C) A type of online scam where attackers disguise themselves as trustworthy organizations (banks, schools, popular apps) to trick people into revealing personal information like passwords, credit card numbers, or account credentials (D) A programming language used to build secure websites, as this directly follows from the underlying principles

22. What are three common 'red flags' that indicate an email might be a phishing attempt?

(A) The email has a company logo, uses professional language, and includes a phone number, and this principle applies across similar situations (B) The email was sent during business hours, has correct spelling, and includes an unsubscribe link, and this has been consistently demonstrated in practice (C) Red flags include: (1) urgent language pressuring immediate action ('Your account will be closed in 24 hours!'), (2) a

sender email address that doesn't match the claimed organization (e.g., 'support@amazon-security.com' instead of '@amazon.com'), and (3) requests for sensitive information like passwords or credit card numbers via email (D) The email is from someone you know, has an attachment, and was sent from a Gmail address, and this principle applies across similar situations

23. You receive an email that appears to be from your school saying: 'Important: Click here to update your student portal password before Friday or you will lose access to your grades.' The sender address is 'admin@school-portal-update.net'. Is this legitimate? Explain your reasoning.

(A) It's definitely fake only because it was sent on a weekend, which aligns with the established guidelines for this age group (B) It's legitimate because it mentions your school and has a specific deadline, since this follows the recommended approach for young people (C) It's legitimate because only your school would know about your student portal, which is consistent with evidence-based health education (D) This is likely phishing. Red flags: the sender domain 'school-portal-update.net' doesn't match the school's actual domain, it creates urgency with a deadline and a threat of losing access, and schools typically communicate password updates through official channels — not via email links. You should verify by contacting the school IT department directly

24. What is 'smishing' and how does it differ from regular phishing?

(A) Smishing is when someone sends too many text messages to crash your phone, which is the most common explanation for this phenomenon (B) Smishing is a type of phishing that only targets smartphones by hacking their cameras, which is why this approach is recommended by experts (C) Smishing is phishing conducted through SMS text messages instead of email. Attackers send texts that appear to be from banks, delivery services, or government agencies, containing links to fake websites designed to steal personal information (D) Smishing is a combination of 'smart' and 'fishing' and only happens on smart TVs, which is the most common explanation for this phenomenon

25. A pop-up appears while you're browsing: 'WARNING! Your computer is infected with 5 viruses! Call 1-800-555-HELP immediately or your data will be destroyed!' What type of scam is this?

(A) This is a legitimate security warning from your operating system that should be taken seriously, and this is the standard approach used in most cases (B) This is a normal advertisement for antivirus software that all websites display, as this is what research and standard practice suggests (C) This is a 'tech support scam' or 'scareware' — a fake warning designed to frighten you into calling a number where scammers will ask for remote access to your computer or payment for unnecessary 'repairs.' Real antivirus software never uses browser pop-ups to report infections (D) This is a real virus warning and you should call the number immediately to save your

computer, and this is the standard approach used in most cases

26. What is a 'fake website' (spoofed site) and how can you tell the difference between a real website and a convincing copy?

(A) Fake websites are impossible to create because web addresses are protected by law (B) You can tell a fake website by its color scheme — real websites always use blue, and this principle applies across similar situations (C) A fake website is a copy of a legitimate site designed to steal login credentials or payment information. You can spot fakes by checking: the URL carefully (amazom.com vs amazon.com), looking for HTTPS, examining the domain spelling, checking for poor design quality, and verifying through a search engine rather than clicking links (D) Fake websites always have visible 'THIS IS FAKE' warnings placed by the internet provider, as this is what research and standard practice suggests

Write the answer

27. You see an ad on social media: 'Congratulations! You've been selected to receive a FREE iPhone 16! Just enter your shipping address and credit card (for \$1.99 shipping only).' Why is this a scam?

Answer: _____

28. What is 'spear phishing' and why is it more dangerous than regular phishing?

Answer: _____

29. A stranger in an online game tells you they work for the game company and can give you free premium currency if you share your login details. How should you respond?

Answer: _____

30. Explain the 'grandparent scam' and what psychological tactic makes it effective.

Answer: _____

Match each question to its answer

1. What is a 'catfish' in the online world? →

2. Compare these two messages and identify which is more likely to be a scam:

Message A: 'Dear [Your Name], your Amazon order #302-7891234 has been delayed. Track your package at amazon.com/tracking.'

Message B: 'URGENT: Your Amazon account has been locked! Click here NOW to verify: <http://amazon-verify-account.suspicious-domain.com/login>' →

3. What is 'pharming' and how does it differ from phishing? →

4. A YouTube comment says: 'I found a glitch in Minecraft that gives unlimited diamonds! Download the mod from this link: bit.ly/minecraft-diamonds-free.' Evaluate

this for safety. →

5. What is 'social proof' and how do scammers use it to make their schemes more believable? →

(A) This is almost certainly malware disguised as a game mod. Red flags: promise of cheats/exploits, a shortened URL hiding the real destination, distribution through YouTube comments instead of official mod platforms, and targeting gamers' desire for in-game advantages. The download likely contains a virus, keylogger, or ransomware

(B) Social proof is the psychological tendency to trust something more when others appear to trust it. Scammers create fake reviews, fabricated testimonials, fake follower counts, and bot comments saying 'This worked for me!' to make their scam look legitimate and popular

(C) Message B is more likely a scam. Red flags: urgency ('URGENT', 'NOW'), threatening language ('locked'), and the URL contains 'suspicious-domain.com' — not Amazon's real domain. Message A is calmer, uses a specific order number, and directs to amazon.com's actual domain

(D) A catfish is someone who creates a fake online identity — using stolen photos, made-up personal details, and false stories — to deceive others into forming a relationship or friendship based on lies, often to manipulate, scam, or exploit the victim

(E) Pharming redirects you to a fake website even when you type the correct URL, by corrupting the DNS system (the internet's address book) on your computer or network. Unlike phishing which requires you to click a link, pharming can trick you without any action on your part

4. Cyberbullying Prevention and Response

Circle the correct answer

31. What is cyberbullying?

(A) Accidentally sending a message to the wrong person (B) Getting a low score on an online game (C) Any argument that happens online between two people (D) Using digital devices to repeatedly and intentionally harass, threaten, or humiliate someone

32. Which of the following is an example of cyberbullying?

(A) Disagreeing with someone's opinion in a group chat (B) Creating a fake social media account to post embarrassing things about a classmate (C) Beating someone in an online multiplayer game (D) Not accepting a friend request from someone you don't know

33. What does the term 'upstander' mean in the context of cyberbullying?

(A) A teacher who punishes the bully (B) Someone who watches bullying happen without getting involved (C) The person doing the bullying (D) Someone who speaks up or takes action to support a person being bullied

34. Why is cyberbullying sometimes considered more harmful than in-person bullying?

(A) Because there are no laws against cyberbullying (B) It can happen 24/7, reach a large audience instantly, and leave a permanent digital record (C) Because cyberbullies are always older than their targets (D) Because online words hurt more than spoken words

35. Marcus notices that every time he posts in the class group chat, three classmates immediately respond with laughing emojis and mocking comments. This has happened for two weeks. What type of cyberbullying is Marcus experiencing?

(A) Trolling — posting random jokes to get attention (B) Catfishing — pretending to be someone else online (C) Flaming — a one-time angry outburst in an argument (D) Harassment — repeated hostile messages targeting a specific person

36. Aisha's friend sends her a screenshot showing that someone created an Instagram account using Aisha's photos and name, posting mean things to other students. What should Aisha do FIRST?

(A) Confront the person she suspects made the account in person (B) Save screenshots as evidence, then report the fake account to Instagram and tell a trusted adult (C) Create a fake account of the suspected bully as revenge (D) Delete all her own social media accounts immediately

Write the answer

37. A classmate sends Jordan a private message saying, 'Everyone hates you. You should just stop coming to school.' Jordan feels hurt but isn't sure if this counts as cyberbullying since it was 'just one message.' Is this cyberbullying? Why or why not?

Answer: _____

38. Three different types of cyberbullying are described below. Which correctly matches each scenario to its type?

Scenario A: Sharing someone's private diary entries in a group chat without permission.

Scenario B: Deliberately leaving one person out of every online group and game invite.

Scenario C: Sending threatening messages saying 'Watch your back at school tomorrow.'

Answer: _____

39. A school is considering three anti-cyberbullying programs:

Program A: Install monitoring software on all student devices to flag mean messages.

Program B: Teach empathy workshops and upstander training, plus create an anonymous reporting system.

Program C: Ban all social media and messaging apps on the school network.

Which program would likely be MOST effective at reducing cyberbullying long-term?

Answer: _____

40. Lena sees a group of classmates posting mean comments on another student's TikTok video. She wants to be an upstander but feels nervous. Which combination of actions would be MOST effective while keeping Lena safe?

Answer: _____

Match each question to its answer

1. What is 'exclusion' as a form of cyberbullying? →

2. Why might someone who cyberbullies others do so even though they wouldn't bully someone face-to-face? →

3. What is 'doxing'? →

4. How does the 'screenshot culture' of social media make cyberbullying harder to escape? →

5. Tyler receives a text from an unknown number with a photo of him at the park, along with the message: 'I know where you go after school.' What should Tyler do? →

(A) Even deleted messages can live forever as screenshots that get shared beyond the original audience

(B) Deliberately and repeatedly leaving someone out of online groups, chats, or gaming sessions

(C) Do not respond, save the message as evidence, show it to a parent or guardian immediately, and consider contacting local authorities

(D) The online disinhibition effect — screens create psychological distance, making people feel anonymous and detached from consequences

(E) Publicly revealing someone's private personal information online without their consent

5. Privacy and Personal Information

Circle the correct answer

41. What is personally identifiable information (PII)?

(A) Any data that can be used to identify a specific individual, such as full name, address, phone number, or Social Security number (B) Information that is already public on social media, and this has been consistently demonstrated in practice (C) Your opinions and preferences about products, which is why this approach is recommended by experts (D) Only information you type into a computer, and this principle applies across similar situations

42. What is a privacy policy?

(A) A promise that a website will never collect any information about you (B) A setting on your phone that blocks all apps from working (C) A government law that makes it illegal to use the internet (D) A legal document that explains how a company collects, uses, stores, and shares your personal data

43. Why do many apps and websites offer free services?

(A) Because it costs nothing to run servers and develop software (B) Because the government pays technology companies to provide free services (C) Because the companies are charities that want to help people (D) They collect and monetize user data through targeted advertising — the user's attention and data are the product being sold

44. What is the difference between data collection and data sharing?

(A) Collection only happens on computers while sharing only happens on phones, and this principle applies across similar situations (B) They are the same thing — both mean storing data on a server, and this has been consistently demonstrated in practice (C) Collection is legal but sharing is always illegal, as this is what research and standard practice suggests (D) Collection is gathering information directly from users; sharing is providing that collected data to third parties like advertisers, partners, or data brokers

45. Nadia downloads a flashlight app that requests access to her contacts, location, microphone, and camera. What should Nadia conclude about this app?

(A) The app requests extra permissions in case it adds features later (B) The app needs location access to determine if it's dark outside (C) The permissions far exceed what a flashlight needs — the app is likely collecting unnecessary data and should not be trusted (D) All apps need these permissions to function properly on modern phones

46. Omar is signing up for a new gaming platform. The signup form asks for his full name, birthdate, school name, home address, phone number, and parent's email. Which pieces of information should Omar provide, and which should he avoid?

(A) Provide fake information for everything including the email address, as this is what research and standard practice suggests (B) Provide only what's necessary: a username (not real name), parent's email for account verification. Avoid sharing

school name, home address, and phone number — these are unnecessary for gaming and create safety risks (C) Provide everything — gaming platforms are always safe and need all this information, and this principle applies across similar situations (D) Provide nothing — creating any online account is always dangerous, and this principle applies across similar situations

Write the answer

47. Elena posts a vacation photo on Instagram while away from home. She tags the hotel location and captions it 'Gone for two weeks! 🌴' What privacy risks has Elena created?

Answer: _____

48. A company's privacy policy states: 'We may share anonymized and aggregated data with third-party partners for research and marketing purposes.' However, research shows that 'anonymized' data can often be re-identified. What is re-identification, and why does it make this policy statement misleading?

Answer: _____

49. Compare COPPA (Children's Online Privacy Protection Act) and GDPR (General Data Protection Regulation) regarding children's privacy:

COPPA: U.S. law, protects children under 13, requires parental consent for data collection.

GDPR: EU law, protects everyone, extra protections for children under 16, right to erasure.

Which law provides stronger privacy protections for a 14-year-old, and why?

Answer: _____

50. Two students debate whether location tracking on phones should be allowed:

Student A: 'Location tracking is great — it helps find lost phones, gives directions, and lets parents know kids are safe.'

Student B: 'Location tracking is dangerous — companies build detailed profiles of everywhere you go, and that data can be sold or hacked.'

Who has the stronger argument?

Answer: _____

Match each question to its answer

1. What is a data broker? →
2. What are cookies in the context of web browsing? →
3. Explain why the phrase 'I have nothing to hide, so I don't need privacy' is a flawed argument. →
4. How does 'browser fingerprinting' track users even when they block cookies? →
5. Jaylen wants to use a VPN (Virtual Private Network) for privacy. His friend says VPNs make you 'completely invisible online.' Evaluate this claim. →

(A) Partially true but misleading — a VPN encrypts traffic and hides your IP address from websites, but the VPN provider can still see your activity, and you remain trackable through account logins, browser fingerprinting, and cookies

(B) It collects unique combinations of device characteristics — browser version, installed fonts, screen resolution, graphics card, time zone — that together create a unique identifier without storing anything on the device

(C) Privacy isn't about hiding wrongdoing — it's a fundamental right that protects against discrimination, manipulation, power imbalances, and the chilling effect on free expression. Everyone has information they rightfully keep private

(D) Small text files that websites store on your device to remember information about your visit, such as login status, preferences, and browsing activity

(E) A company that collects personal information from various sources and sells compiled profiles to other businesses, advertisers, or individuals

6. Social Media Literacy and Digital Wellness

Circle the correct answer

51. What is an algorithm in the context of social media?

(A) A settings menu where you select your favorite topics, which is why this approach is recommended by experts (B) A set of rules and calculations that determines what content appears in your feed based on your past behavior, interests, and engagement patterns (C) The person at the company who manually chooses what you see, and this is the standard approach used in most cases (D) A type of computer virus that spreads through social media, and this is the standard approach used in most cases

52. What is a 'filter bubble'?

(A) A parental control that limits which websites children can visit (B) When algorithms show you only content that matches your existing beliefs and interests, isolating you from diverse perspectives (C) A spam filter that blocks unwanted emails (D) A photo filter that makes everyone look the same

53. Why do social media platforms use 'infinite scroll' instead of pagination (numbered pages)?

(A) Infinite scroll removes natural stopping points, making it harder for users to decide to stop browsing — it exploits the brain's tendency to keep consuming when there's no clear endpoint (B) Because infinite scroll loads pages faster than numbered pages (C) Because users asked social media companies to remove page numbers (D) Because numbered pages are too expensive for companies to program

54. What is the 'social comparison trap' on social media?

(A) A game on social media where you compete for the most likes, as this is what research and standard practice suggests (B) The tendency to compare your everyday life to other people's carefully curated highlight reels, leading to feelings of inadequacy even though the comparison is unfair (C) A scam where people pretend to be celebrities to steal your money, and this principle applies across similar situations (D) A feature that ranks users by popularity, and this is the standard approach used in most cases

55. Maya notices she feels anxious when she doesn't check her phone for more than 30 minutes. She gets a rush of excitement when she sees notifications, but feels empty shortly after. What psychological pattern is this describing?

(A) An allergic reaction to the phone's screen radiation, and this principle applies across similar situations (B) Normal behavior — everyone checks their phone every 30 minutes, which is the most common explanation for this phenomenon (C) A phone virus that sends fake notifications to trick users, which is why this approach is recommended by experts (D) A variable reward loop — unpredictable notifications create dopamine spikes similar to slot machines, and the anxiety between checks resembles withdrawal from intermittent reinforcement

56. Carlos has 1,200 followers on Instagram but only interacts regularly with about 15 people. He spends 2 hours daily maintaining his online presence for followers he doesn't know personally. Using the concept of 'Dunbar's number' (humans can maintain about 150 meaningful social connections), analyze Carlos's situation.

(A) 1,200 followers is below average, so Carlos should spend more time gaining followers, which is the most common explanation for this phenomenon (B) Carlos is investing significant time maintaining superficial connections far beyond his meaningful relationship capacity. The 1,185 followers he doesn't interact with provide social validation metrics but not genuine connection — he's optimizing for numbers rather than relationship quality (C) Dunbar's number doesn't apply to social media because online friendships don't count (D) Carlos needs more followers to reach Dunbar's number of 150 meaningful connections, and this principle applies across similar situations

Write the answer

57. What is 'doomscrolling'?

Answer: _____

58. Explain why social media platforms show you content that makes you angry or outraged, even though negative emotions seem bad for user experience.

Answer: _____

59. Aiden sees an Instagram post of a friend's 'perfect' beach vacation. He feels jealous and inadequate about his own summer. Later, he learns his friend was actually stressed during the trip because of family arguments and spent 45 minutes staging and editing the beach photo. What does this reveal about social media content?

Answer: _____

60. A new social media platform advertises: 'No algorithms! You see posts in chronological order from people you follow.' Is this platform automatically better for digital wellness?

Answer: _____

Match each question to its answer

1. What does FOMO stand for, and why is it relevant to social media? →

2. What is 'persuasive design' in technology? →

3. How do 'streaks' on platforms like Snapchat use psychology to keep users engaged? →

4. Zara's screen time report shows she spends 4 hours daily on social media. She decides to cut it to 1 hour by going 'cold turkey' — deleting all social media apps immediately. Her friend suggests a gradual approach instead — reducing by 30 minutes per week. Which strategy is more likely to succeed, and why? →

5. TikTok's algorithm is known for being exceptionally good at predicting what users want to watch, sometimes within minutes of a new user joining. Analyze how this rapid personalization could be both beneficial and harmful for a 12-year-old user. →

(A) Benefits: quickly surfaces genuinely interesting educational and creative content, connects users with communities sharing their interests. Harms: can rapidly push users toward extreme content through radicalization pathways, creates deeply personalized addiction loops that are harder to break, and a 12-year-old lacks the metacognitive awareness to recognize algorithmic manipulation

(B) Design techniques intentionally built into apps and websites to influence user behavior, keep users engaged longer, and encourage specific actions like sharing, purchasing, or returning frequently

(C) Streaks exploit loss aversion — people fear losing their accumulated streak more than they value maintaining it. The longer the streak, the greater the perceived loss, creating an obligation to open the app daily

(D) The gradual approach is more likely to succeed because habits built over time

resist sudden change — reducing incrementally allows the brain to adjust, find replacement activities, and build sustainable new routines without the willpower depletion of cold turkey

(E) Fear Of Missing Out — the anxiety that others are having rewarding experiences without you. Social media amplifies FOMO by constantly showing what friends are doing, making you feel left out

7. Critical Thinking and Misinformation Online

Circle the correct answer

61. What is the difference between misinformation and disinformation?

(A) Misinformation is false information shared without intent to deceive (the sharer believes it's true); disinformation is false information deliberately created and spread to mislead people (B) Misinformation is about politics while disinformation is about science, and this is the standard approach used in most cases (C) Misinformation comes from social media while disinformation comes from news websites, as this is what research and standard practice suggests (D) They mean the same thing — both refer to any false information, and this has been consistently demonstrated in practice

62. What is 'confirmation bias' and how does it relate to misinformation?

(A) Confirmation bias is the tendency to seek, interpret, and remember information that confirms existing beliefs while ignoring contradictory evidence — it makes people more likely to believe and share misinformation that aligns with what they already think (B) A type of bias that only affects unintelligent people, and this has been consistently demonstrated in practice (C) A bias in computer algorithms that confirms user accounts, and this is the standard approach used in most cases (D) The tendency to only read confirmed, fact-checked news sources, and this is the standard approach used in most cases

63. What is 'lateral reading' as a fact-checking technique?

(A) Only reading the sidebar links on a webpage, and this is the standard approach used in most cases (B) Instead of evaluating a website by reading its content deeply, you open new tabs to search what OTHER sources say about the site, its author, and its claims — reading 'laterally' across multiple sources rather than 'vertically' within one source (C) Scrolling through comments to see if readers agree with the article, and this principle applies across similar situations (D) Reading an article from left to right instead of top to bottom, making this the most widely accepted explanation

64. Why does misinformation spread faster than accurate information on social media?

(A) Because accurate information is boring and nobody reads it, based on the current recommendations from health professionals (B) Misinformation is often more novel, emotionally provocative, and surprising than facts — it triggers stronger emotional reactions that drive sharing. Algorithms amplify engaging content regardless of accuracy, and the human brain processes emotional content before analytical evaluation (C) Because social media companies deliberately promote false information, since this follows the recommended approach for young people (D) Because fact-checking organizations are too slow to catch up, which aligns with the established guidelines for this age group

65. A viral social media post claims: 'Scientists have proven that eating chocolate every day prevents cancer. Study published in the Journal of Health Research.' You want to verify this claim. Apply the SIFT method (Stop, Investigate the source, Find better coverage, Trace claims) to evaluate it.

(A) Check if the post has many likes and shares — popular posts are usually accurate, making this the most widely accepted explanation, since this follows the recommended approach for young people (B) The claim mentions a journal, so it must be scientifically verified and safe to share, as this directly follows from the underlying principles, according to the standard health and wellness practices (C) Ask your friends if they think the claim sounds reasonable, making this the most widely accepted explanation, which aligns with the established guidelines for this age group (D) Stop — don't share yet. Investigate — search for 'Journal of Health Research' (is it a reputable peer-reviewed journal or a predatory journal?). Find better coverage — search the claim on fact-checking sites and legitimate health news. Trace — find the original study to check if it actually says what the post claims (likely it found a correlation, not that chocolate 'prevents' cancer)

66. Your aunt shares a news article on Facebook with the headline: 'BREAKING: Local Water Supply Contaminated — Officials Covering Up!' The article comes from a website called 'TruthPatriotNews.com' that you've never heard of. Using lateral reading, what steps would you take to evaluate this claim before deciding whether to worry?

(A) Open new tabs to: (1) search the website name — check if it's a known misinformation site, (2) search the specific claim on local news outlets and government health sites, (3) check if any established news organizations are reporting the same story, (4) look for official water quality reports from local authorities. If only this one unknown site reports it, the claim is likely false (B) Check the comments section to see if other readers believe it, and this principle applies across similar situations, which is consistent with evidence-based health education (C) Read the full article carefully — if it has lots of details, it's probably true, making this the most widely accepted explanation, according to the standard health and wellness practices (D) Share it with your family immediately because water safety is too important to

wait, since this follows the recommended approach for young people

Write the answer

67. What is a 'deepfake'?

Answer: _____

68. A YouTube video titled 'The REAL Reason Schools Don't Want You to Know This' has 2 million views and thousands of positive comments. Does its popularity indicate that the information is accurate?

Answer: _____

69. Identify the propaganda technique used in each statement:

A: 'Every real American supports this policy.'

B: 'Dr. Smith, a famous heart surgeon, says this energy drink is the healthiest option.'

C: 'This politician is just like Hitler.'

Answer: _____

70. What is the 'illusory truth effect' and why is it dangerous in the context of social media?

Answer: _____

Match each question to its answer

1. What is a 'predatory journal' or 'predatory publisher'? →

2. What is 'astroturfing' in the context of online information? →

3. An image circulates on social media showing a politician shaking hands with a known criminal. Outraged comments flood in. However, investigation reveals the image is from a public event where the politician met hundreds of people, and the criminal's conviction happened years after the photo was taken. What manipulation technique does this represent? →

4. During a natural disaster, you see the following posts on social media:

Post A: A verified news organization reporting 50 homes damaged with a source from local emergency services.

Post B: A user claiming 5,000 homes destroyed with a dramatic video that reverse image search shows is from a different country two years ago.

Post C: A local resident posting their own video of flooding on their street.

Rank these from most to least reliable and explain your reasoning. →

5. What is the 'Gish Gallop' technique, and how is it used in online debates to overwhelm critical thinking? →

(A) The Gish Gallop floods an opponent with a large number of arguments, claims, and questions in rapid succession — regardless of accuracy. It overwhelms because each false claim takes far more effort to debunk than to make, making it impossible to address everything and creating the illusion that the unanswered claims are valid

(B) Most reliable: Post A (verified source, cites official emergency services), then Post C (firsthand eyewitness but limited to one location), then Post B (uses misattributed footage from a different event, wildly exaggerated numbers). Post B is actively harmful disinformation

(C) The practice of masking a sponsored message or organized campaign as spontaneous grassroots activity — making corporate, political, or state-backed campaigns appear to be organic public opinion

(D) A fraudulent academic publisher that charges authors fees to publish their work but provides little or no peer review, editorial oversight, or quality control — allowing unreliable or fabricated research to appear 'published'

(E) Decontextualization — taking a real image out of its original context to create a misleading narrative. The photo is authentic but the implied meaning (the politician knowingly associates with criminals) is false

8. Master Digital Citizen Capstone

Circle the correct answer

71. What is 'digital citizenship'?

(A) Being a citizen of a country that has internet access, as this is what research and standard practice suggests (B) Knowing how to code websites and apps, as this directly follows from the underlying principles (C) The responsible, ethical, and informed use of technology — encompassing online safety, privacy awareness, respectful communication, critical information evaluation, and understanding your rights and responsibilities in digital spaces (D) Having an account on social media, and this has been consistently demonstrated in practice

72. Name the five pillars of digital citizenship covered in this course.

(A) Digital identity and footprint, password security and account protection, online safety (scams, phishing, cyberbullying), privacy and personal information, and media/information literacy (misinformation, social media awareness) (B) Coding, gaming, social media, streaming, and online shopping, making this the most widely accepted explanation (C) Hardware, software, networks, databases, and programming, and this is the standard approach used in most cases (D) Facebook, Instagram, TikTok, YouTube, and Snapchat, and this principle applies across similar situations

73. Explain why digital citizenship skills become MORE important, not less, as technology advances.

(A) Digital citizenship becomes less important because technology companies handle safety automatically, according to the standard health and wellness practices
(B) It becomes less important because people naturally learn to use technology safely over time, since this follows the recommended approach for young people
(C) As technology becomes more powerful and integrated into daily life, the stakes increase: AI makes misinformation more convincing, IoT expands surveillance, social media's psychological effects deepen, and digital decisions have more real-world consequences. Skills that protect against manipulation, privacy invasion, and online harm must evolve alongside the technology that creates these threats
(D) It stays the same because the basic principles never change, which aligns with the established guidelines for this age group

74. How do digital footprint, privacy, and cyberbullying intersect? Provide a scenario where all three issues are connected.

(A) Footprint only relates to privacy, and cyberbullying is a separate issue entirely, which is why this approach is recommended by experts, since this follows the recommended approach for young people
(B) These concepts only connect when someone is using social media, as this is what research and standard practice suggests, which is consistent with evidence-based health education
(C) They're deeply interconnected: your digital footprint determines what information is available about you (privacy exposure), which cyberbullies can exploit to target you more effectively. Example: a student shares their school name in a gaming profile (footprint), which reveals their location (privacy gap), which a cyberbully uses to make real-world threats ('I know where you go to school'). Conversely, cyberbullying creates a negative digital footprint for the target through spread of harmful content
(D) They are three completely separate topics that don't affect each other, and this principle applies across similar situations, based on the current recommendations from health professionals

75. Jaylen receives a direct message from an account claiming to be a talent scout: 'I saw your basketball highlights on TikTok! I work with Nike and want to sponsor you. Send me your full name, school address, and parent's phone number so I can mail a contract. Don't tell anyone yet — this is an exclusive offer!' Apply your digital citizenship knowledge to identify every red flag in this message.

(A) Only the school address is a concern — the rest of the information is safe to share, which is the most common explanation for this phenomenon
(B) This is safe as long as Jaylen doesn't send money, which is why this approach is recommended by experts, which aligns with the established guidelines for this age group
(C) Red flags: (1) Unsolicited contact from a stranger requesting PII (full name, school address, parent's phone). (2) Urgency and exclusivity pressure ('don't tell anyone yet'). (3) Legitimate companies don't recruit minors through DMs. (4) Real sponsorships go

through official channels with parental involvement from the start. (5) Requesting physical addresses via DM is a safety concern. (6) 'Don't tell anyone' is the #1 grooming tactic — isolating the target from trusted adults. (7) No verifiable company contact information provided (D) This seems legitimate because Nike does sponsor young athletes, since this follows the recommended approach for young people

76. A viral TikTok claims that a new phone app can 'delete your entire digital footprint with one tap.' The video has 5 million views, hundreds of positive comments, and shows a before/after of Google search results. Evaluate this claim using skills from multiple units (privacy, misinformation, and persuasive design).

(A) Only the privacy claim is questionable — the rest seems legitimate, and this has been consistently demonstrated in practice, which is consistent with evidence-based health education (B) If it's on TikTok with that many views, TikTok would have removed it if it were false, which is why this approach is recommended by experts, since this follows the recommended approach for young people (C) The app probably works because it has 5 million views and positive reviews, which aligns with the established guidelines for this age group (D) Privacy analysis: Complete footprint deletion is technically impossible — data exists on thousands of servers, in backups, screenshots, and data broker databases. Misinformation analysis: The before/after could be easily faked or show cached vs non-cached results; the claim is extraordinary and requires extraordinary evidence. Persuasive design analysis: The viral spread, positive comments (possibly bot-generated), and too-good-to-be-true promise follow typical scam patterns. The app likely harvests MORE data rather than deleting existing data

Write the answer

77. What is the relationship between algorithms, filter bubbles, and the spread of misinformation?

Answer: _____

78. Emma's school implements a new policy: students must use a school-issued Chromebook for all schoolwork, the school monitors all activity on the device (including after school hours), search history is reviewed weekly by administrators, and any 'concerning' activity triggers a parent notification. Analyze this policy from multiple digital citizenship perspectives: privacy rights, safety benefits, and potential harms.

Answer: _____

79. A classmate starts a petition on Change.org to get a teacher fired, based on a 15-second video clip that appears to show the teacher yelling at a student. The petition goes viral with 10,000 signatures. However, the full 5-minute video shows the teacher calmly managing a dangerous situation where a student was about to harm

themselves, and the 'yelling' was the teacher urgently telling other students to get help. Analyze this situation through the lenses of digital footprint, misinformation, mob mentality, and real-world consequences.

Answer: _____

80. What is the 'paradox of tolerance' as it applies to online spaces?

Answer: _____

Match each question to its answer

1. What does the term 'digital literacy' encompass beyond basic technology skills? →

2. Why is the concept of 'consent' important across ALL areas of digital citizenship — not just privacy? →

3. Zara discovers that her best friend's Instagram account has been hacked. The hacker is posting offensive content and messaging Zara's friend's followers pretending to be her. Zara knows her friend's recovery email and has her phone number. Create a step-by-step action plan using knowledge from security, privacy, and relationship management. →

4. A new AI chatbot marketed to teens promises to be a 'perfect friend who always listens.' It's free, requires creating an account with age and interests, and the conversations feel remarkably human. Analyze this product from privacy, digital wellness, and ethical perspectives. →

5. Your school newspaper publishes an article online about a student's academic achievement. The article includes the student's full name, grade, age, and photo. Three years later, the now-high-school student applies for a job and the employer finds this article. Is this a digital footprint issue, a privacy issue, both, or neither? Explain the complexity. →

(A) Step 1: Contact the friend immediately via phone call (not DM, since the account is compromised) to confirm they know about the hack. Step 2: Help the friend report the compromised account to Instagram through the official 'hacked account' recovery flow. Step 3: The friend should change passwords on all accounts that used the same password (credential stuffing risk). Step 4: Alert mutual friends that the account is hacked so they don't interact with the hacker. Step 5: Enable 2FA on all recovered accounts. Step 6: Document the hacker's posts as evidence in case of identity theft or further harassment

(B) Privacy: The chatbot collects intimate personal data (emotions, problems, secrets) from minors who may not realize conversations are stored and analyzed. Digital wellness: It may substitute for real human connection, and the 'always available' nature could deepen technology dependence. Ethics: The company monetizes children's emotional vulnerability — the chatbot is 'free' because the data is the product. Additionally, an AI 'friend' that never disagrees or challenges you is an unhealthy relationship model

(C) Both — and they're intertwined. Digital footprint: the article creates a permanent, searchable record the student had no control over. Privacy: a minor's personal information (name, age, photo, school) was published online with potentially inadequate consent considerations. The complexity: the article was positive and published by a trusted institution, yet it still created privacy exposure. This shows that even well-intentioned content contributes to a digital footprint that follows people across life stages

(D) Digital literacy includes the ability to critically evaluate online information, understand how platforms and algorithms work, protect personal privacy, communicate respectfully and effectively online, create content responsibly, and recognize manipulation techniques — not just knowing how to use devices and software

(E) Consent applies everywhere: sharing someone's photo (digital footprint), accessing their account (security), forwarding their private messages (privacy), including them in group chats (relationships), and using their creative work (intellectual property). In every digital interaction, the question 'did this person agree to this?' should guide ethical behavior

9. Safety & Preparedness

Circle the correct answer

81. What should you do first if your clothes catch fire?

(A) Run to find water (B) Wave your arms to put it out (C) Take off the clothing immediately (D) Stop, drop, and roll

82. How often should smoke alarm batteries be tested?

(A) Only when they beep (B) Once a year (C) At least once a month (D) Every five years

83. What is the recommended way to escape a smoke-filled room?

(A) Open a window and wait (B) Run through the smoke quickly (C) Crawl low under the smoke (D) Stand up and cover your mouth

84. What number should you call in a fire emergency in the United States?

(A) 311 (B) 911 (C) 411 (D) 611

85. What device in your home warns you about smoke or fire?

(A) Carbon monoxide detector (B) Thermostat (C) Security camera (D) Smoke alarm

86. What should every family create and practice for fire emergencies?

(A) A phone tree for neighbors (B) A list of valuable items to save (C) A home fire escape plan (D) A fire extinguisher collection

Write the answer

87. Why should you feel a closed door with the back of your hand before opening it during a fire?

Answer: _____

88. Why is it important to have two escape routes from every room?

Answer: _____

89. What does "Get Out, Stay Out" mean in fire safety?

Answer: _____

90. Why do firefighters recommend sleeping with your bedroom door closed?

Answer: _____

Match each question to its answer

1. How does a fire extinguisher work to put out small fires? →

2. You smell smoke while sleeping and your smoke alarm is beeping. What should you do first? →

3. Your family is creating a fire escape plan. What should you pick as a meeting place? →

4. You are cooking and a small grease fire starts in a pan. What should you do? →

5. You are visiting a hotel and want to be prepared for a fire. What should you do when you first arrive? →

(A) It sprays a substance that removes heat or oxygen from the fire

(B) Locate the nearest fire exits and count doors to the stairwell

(C) A specific spot outside the home, like a mailbox or tree

(D) Roll out of bed and crawl to your planned escape route

(E) Slide a lid over the pan and turn off the burner

10. Safety & Preparedness

Circle the correct answer

91. What is the first step in treating a minor burn?

(A) Cover it with ice directly (B) Cool the burn under cool running water for at least 10 minutes (C) Pop any blisters that form (D) Apply butter to the burn

92. What does the acronym CPR stand for?

- (A) Cardiac pulse restart (B) Chest pressure response (C) Critical patient recovery
(D) Cardiopulmonary resuscitation

93. What should you use to apply pressure to a bleeding wound?

- (A) Your bare hands only (B) Nothing — let it bleed to clean itself (C) A dirty towel is fine (D) A clean cloth or bandage

94. What number should you call for a medical emergency in the United States?

- (A) 411 (B) 211 (C) 911 (D) 311

95. What is a first aid kit?

- (A) A kit that replaces going to the hospital, as this directly follows from the underlying principles (B) A collection of supplies used to treat minor injuries and stabilize serious ones until help arrives (C) A bag of bandages for paper cuts only, as this is what research and standard practice suggests (D) A box of medicine only doctors can use, and this has been consistently demonstrated in practice

96. What does the recovery position look like?

- (A) The person is lying flat on their back (B) The person is standing and leaning against a wall (C) The person is lying on their side with their top leg bent for stability (D) The person is sitting upright with arms crossed

Write the answer

97. Why should you wash a cut with clean water before bandaging it?

Answer: _____

98. Why is it important to wear gloves when helping someone who is bleeding?

Answer: _____

99. Explain why you should NOT remove an object stuck in a wound.

Answer: _____

100. Why should a person with a suspected spinal injury NOT be moved?

Answer: _____

Match each question to its answer

1. What is the purpose of elevating an injured limb above the heart? →

2. Your friend falls off a bike and scrapes their knee badly. It is bleeding but not severe. What should you do? →

3. Someone at a picnic is stung by a bee and says they are allergic. They are having trouble breathing. What should you do? →

4. You find someone unconscious but breathing normally. What position should you

place them in? →

5. A classmate gets a nosebleed during class. How should they handle it? →

- (A) Call 911 immediately and help them use their epinephrine auto-injector if they have one
 - (B) Lean slightly forward and pinch the soft part of the nose for 10-15 minutes
 - (C) To reduce blood flow to the area, which helps slow bleeding and reduce swelling
 - (D) The recovery position — on their side with top leg bent
 - (E) Clean the wound with water, apply gentle pressure with a clean cloth, then bandage it
-

11. Safety & Preparedness

Circle the correct answer

101. What should you do during an earthquake if you are indoors?

- (A) Drop, cover, and hold on under a sturdy piece of furniture
- (B) Lie flat in the middle of the room
- (C) Stand in a doorway
- (D) Run outside immediately

102. Where is the safest place to go during a tornado warning?

- (A) An upstairs bedroom, which is the most common explanation for this phenomenon
- (B) Near a large window to watch, and this principle applies across similar situations
- (C) A basement or an interior room on the lowest floor, away from windows
- (D) Outside in an open field, and this is the standard approach used in most cases

103. What is an emergency supply kit?

- (A) A collection of essential supplies to survive for at least 72 hours after a disaster
- (B) Supplies only needed during hurricanes
- (C) A bag of clothes for a vacation
- (D) A kit that replaces emergency services

104. How many gallons of water per person per day does FEMA recommend storing for emergencies?

- (A) Two gallons per person per week
- (B) One gallon per person per day
- (C) Five gallons per family per day
- (D) Half a gallon per person per day

105. What does a tornado watch mean?

- (A) A tornado has been spotted — take shelter now
- (B) The tornado season has officially started
- (C) Tornadoes are no longer a threat
- (D) Conditions are favorable for tornadoes to develop — be prepared

106. What natural disaster is measured using the Richter scale or moment magnitude scale?

- (A) Earthquake (B) Tsunami (C) Tornado (D) Hurricane

Write the answer

107. Why should families have a communication plan before a disaster strikes?

Answer: _____

108. Explain why you should NOT drive through flooded roads.

Answer: _____

109. Why is it important to include copies of important documents in an emergency kit?

Answer: _____

110. How does an earthquake cause a tsunami?

Answer: _____

Match each question to its answer

1. Why should you have a battery-powered or hand-crank radio in your emergency kit?

→

2. An earthquake starts while you are in a classroom. Describe what you should do. →

3. Your family needs to build a 72-hour emergency kit. Name the most critical items to include. →

4. A hurricane warning has been issued for your area. Your family decides to evacuate. What should you do before leaving? →

5. You are outdoors when a tornado siren goes off but there are no buildings nearby. What should you do? →

(A) Power outages during disasters disable TVs and internet, but emergency radio broadcasts continue

(B) Secure the home, grab your emergency kit and documents, follow the designated evacuation route

(C) Drop under your desk, cover your head and neck, hold on to the desk legs until shaking stops

(D) Lie flat in the lowest spot you can find, like a ditch, and cover your head with your hands

(E) Water, non-perishable food, flashlight, batteries, first aid kit, medications, phone charger, and important documents

12. Safety & Preparedness

Circle the correct answer

111. What is a strong password?

(A) A long, unique combination of letters, numbers, and symbols that is hard to guess (B) The word "password" with a capital P, which is the most common explanation for this phenomenon (C) Your birthday in number form, which is why this approach is recommended by experts (D) Your name followed by 123, as this is what research and standard practice suggests

112. What is phishing?

(A) A security feature that protects your email, as this directly follows from the underlying principles (B) A scam where someone pretends to be a trusted source to trick you into sharing personal information (C) A way to speed up your internet, and this is the standard approach used in most cases (D) A type of online fishing game, which is why this approach is recommended by experts

113. Who should you tell if a stranger online asks for your personal information?

(A) A trusted adult, like a parent or teacher (B) The stranger, so they stop asking (C) Your online friends (D) No one — it is probably fine

114. What is cyberbullying?

(A) Using a computer for homework (B) Using technology to harass, threaten, embarrass, or target another person (C) Sending too many text messages (D) Playing video games competitively

115. What personal information should you NEVER share online with strangers?

(A) Full name, address, school name, phone number, and passwords (B) Your favorite color, and this is the standard approach used in most cases (C) What music you like, as this directly follows from the underlying principles (D) Your opinion on a movie, as this is what research and standard practice suggests

116. What does a padlock icon in your browser address bar mean?

(A) The website uses encryption (HTTPS) to protect data sent between you and the site (B) The website is blocked by your school (C) Your computer has a virus (D) The website is completely safe and trustworthy

Write the answer

117. Why should you use different passwords for different accounts?

Answer: _____

118. Explain why you should think before you post something online.

Answer: _____

119. How do phishing emails trick people into clicking malicious links?

Answer: _____

120. Why is location sharing on social media potentially dangerous?

Answer: _____

Match each question to its answer

1. What is the difference between a secure website (HTTPS) and an unsecure one (HTTP)? →

2. You receive an email claiming to be from your favorite game company saying your account was hacked. It asks you to click a link and enter your password. What should you do? →

3. A person you only know online wants to meet in real life. What should you do? →

4. You notice a classmate is being cyberbullied in a group chat. What should you do? →

5. You want to create a new account on a website. How should you create a safe username? →

(A) HTTPS encrypts data between your browser and the website; HTTP sends data as plain text anyone can read

(B) Tell a trusted adult and never meet an online stranger alone

(C) Do not click the link — go directly to the game company website by typing the URL yourself, and report the email

(D) Do not participate, save evidence by taking screenshots, support the person being bullied, and tell a trusted adult

(E) Use a creative name that does not include your real name, age, location, or school

13. Long-term Consequences

Circle the correct answer

121. What is a 'digital footprint'?

(A) The physical mark your shoe leaves when you step on a keyboard, which is why this approach is recommended by experts (B) A special type of computer password shaped like a footprint, and this principle applies across similar situations (C) The trail of data and information you leave behind whenever you use the internet — including posts, searches, photos, comments, and account activity (D) A measurement of how fast your internet connection is, as this is what research and

standard practice suggests

122. Maya posted a photo of her new puppy on a social media app. She later deleted the post. Is the photo completely gone from the internet? Why or why not?

(A) No — even though Maya deleted her post, the photo may still exist in the app's backup servers, in friends' screenshots, in cached copies on search engines, or if someone shared or saved it before deletion (B) Yes, deleting a post permanently removes all traces of it from every server and device everywhere (C) Yes, once you delete something online it is legally required to be erased from all databases (D) No, but only because Maya's phone still has the original photo in its camera roll

123. Which of the following is an example of personal information you should NOT share publicly online?

(A) Your opinion about whether cats or dogs make better pets (B) Your home address, school name, phone number, or full birthday (including the year you were born) (C) The name of a movie you recently enjoyed watching (D) Your favorite color or what kind of music you like

124. Liam uses the same username — 'LiamSmith2014Chicago' — on a gaming site, a homework forum, and a social media app. What digital safety problem does this create?

(A) The username reveals his real name (Liam Smith), birth year (2014), and city (Chicago), and using it across multiple platforms lets anyone connect all his accounts and build a detailed profile of him (B) Using the same username is fine because it makes it easier for friends to find him (C) The only problem is that usernames with numbers look unprofessional, making this the most widely accepted explanation (D) The username is too long and might not fit in some text fields, and this is the standard approach used in most cases

125. What does the term 'digital identity' mean?

(A) The serial number on your computer or phone, which is the most common explanation for this phenomenon (B) A special ID card you need to access the internet, which is why this approach is recommended by experts (C) The overall picture of who you are online — built from your usernames, profiles, posts, comments, photos, likes, and how you interact with others across all platforms (D) Your email address and nothing else, making this the most widely accepted explanation

126. Emma wants to create a positive digital footprint. Which of these actions would BEST help her do that?

(A) Sharing her science fair project online, writing encouraging comments on friends' posts, and joining a student volunteer group's page (B) Posting mean jokes about classmates using a fake account so no one knows it's her (C) Downloading as many apps as possible to make her phone look impressive (D) Sharing every detail of her daily routine including where she is at all times

Write the answer

127. Jake's friend dares him to post an embarrassing video of another classmate who fell during gym class. Jake thinks it's funny. What should Jake consider before posting?

Answer: _____

128. Why might colleges and future employers search for your name online before accepting you?

Answer: _____

129. Aisha created accounts on three different apps. On one, she uses her real name and photo. On another, she uses a nickname and an avatar. On the third, she is completely anonymous. Which account is safest for commenting on news articles?

Answer: _____

130. What are 'cookies' in the context of web browsing?

Answer: _____

Match each question to its answer

1. Carlos discovers that a photo he posted two years ago on a gaming forum has been copied and used in a meme that is spreading on social media. He never gave permission for this. What can Carlos learn from this experience? →

2. What is the difference between your 'online reputation' and your 'real-life reputation'? →

3. Priya's teacher asks the class to search their own names online. Priya finds an old blog post from a summer camp website that includes her full name, age, and the city she lives in. What should Priya do? →

4. Tyler says, 'I don't care about my digital footprint because I'm only 11 — it won't matter until I'm an adult.' Why is Tyler wrong? →

5. A new app asks for permission to access your contacts, camera, microphone, location, and photo library during installation. The app is a simple calculator. What should you think about before accepting all these permissions? →

(A) Priya should tell her parent or guardian about the post and ask them to contact the camp website to request the information be removed, since it contains personal details that could compromise her privacy

(B) Once you share content online, you lose control over how others use it — even old posts from years ago can be found, copied, and spread without your permission, so every post should pass the 'would I be okay with this going viral?' test

(C) Tyler's digital footprint starts now and accumulates over time. Things he posts at age 11 will still be searchable when he's 18 and applying to college, meaning years of online behavior build the reputation that future decision-makers will see

(D) A calculator has no legitimate reason to access contacts, camera, microphone, location, or photos — these excessive permission requests suggest the app may be collecting personal data for purposes unrelated to its function, and you should deny unnecessary permissions or not install it

(E) Your online reputation is visible to a much larger audience (potentially the entire internet), persists much longer (possibly forever), and is searchable — while your real-life reputation is limited to people who know you personally and fades over time

14. Long-term Consequences

Circle the correct answer

131. A friend sends you a funny meme that has a classmate's face photoshopped onto an embarrassing image. Your friend asks you to share it with your group chat. What is the best course of action?

- (A) Share it because your friend asked and you don't want to seem like a bad friend
(B) Do not share it — tell your friend that spreading altered images of someone without their consent is hurtful and could be considered cyberbullying, and suggest they delete it too
(C) Share it only to the group chat because a small audience makes it okay
(D) Save it to your phone but don't share it, in case you need it later

132. A friend shares a link to a 'personality quiz' on social media that says it will tell you your Hogwarts house. The quiz asks for your email, birthday, mother's maiden name, and the street you grew up on. Why are these questions suspicious?

- (A) The questions are fine because the quiz needs demographic data for marketing research
(B) The questions are suspicious only because they have nothing to do with Harry Potter
(C) These are normal quiz questions that all personality tests ask for accuracy, as this directly follows from the underlying principles
(D) These questions match common security questions used for account recovery. The quiz is likely designed to harvest answers to security questions — with your email, birthday, mother's maiden name, and childhood street, an attacker could reset passwords on many of your accounts

133. Zoe's friend asks to borrow her gaming account password 'just for one day' to try a game Zoe owns. What should Zoe do?

- (A) Share it but change it after 24 hours which makes it completely safe, and this principle applies across similar situations
(B) Share it because good friends always share everything including passwords
(C) Zoe should not share her password — even with a trusted friend. Sharing passwords gives another person access to personal messages, payment information, and the ability to make purchases or changes under Zoe's name
(D) Share it only over text message because texts are always private and

secure

134. Which of these passwords is the strongest, and why?

- A) Fluffy123
- B) p@ssw0rd!
- C) My-Cat-Loves-Tuna-Sandwiches!
- D) 12345678901234

(A) D) because it has 14 characters which makes it the longest password in the list
(B) C) 'My-Cat-Loves-Tuna-Sandwiches!' — it is the longest (32 characters), uses a passphrase format that is easy to remember but hard to crack, and includes uppercase, lowercase, hyphens, and a symbol
(C) A) because it uses a mix of letters and numbers which is the most important factor
(D) B) because replacing letters with symbols like @ and 0 makes any password uncrackable

135. Rachel's Instagram shows she is on vacation in Hawaii. While she's away, she gets a text from her 'bank' saying: 'We detected unusual login activity from Hawaii on your account. Verify your identity immediately: [link].' What makes this particularly convincing?

(A) The text is legitimate because only her real bank would know she's in Hawaii, which aligns with the established guidelines for this age group
(B) The scammers used information from Rachel's public Instagram posts to make the phishing message seem legitimate — mentioning Hawaii matches her actual location, making the 'unusual activity' warning feel real and urgent. This is spear phishing using publicly available social media data
(C) It's convincing because banks always monitor your Instagram for security purposes, according to the standard health and wellness practices
(D) It's convincing because banks track your phone's GPS and the text confirms your location, since this follows the recommended approach for young people

136. What is personally identifiable information (PII)?

(A) Only information you type into a computer, and this principle applies across similar situations
(B) Information that is already public on social media, and this has been consistently demonstrated in practice
(C) Your opinions and preferences about products, which is why this approach is recommended by experts
(D) Any data that can be used to identify a specific individual, such as full name, address, phone number, or Social Security number

Write the answer

137. A classmate tells you about a website where you can watch new movies for free — movies that are currently in theaters. What risks does this site pose beyond just the legal issue of piracy?

Answer: _____

138. A YouTube video titled 'The REAL Reason Schools Don't Want You to Know This' has 2 million views and thousands of positive comments. Does its popularity indicate that the information is accurate?

Answer: _____

139. What is a privacy policy?

Answer: _____

140. What is 'doxing'?

Answer: _____

Match each question to its answer

1. Omar uses public Wi-Fi at a coffee shop to log into his email. His friend says this is risky. Why? →

2. Explain why social media platforms show you content that makes you angry or outraged, even though negative emotions seem bad for user experience. →

3. What are 'security questions' (like 'What is your mother's maiden name?') and why are they actually a weak form of security? →

4. Why might someone who cyberbullies others do so even though they wouldn't bully someone face-to-face? →

5. When a company experiences a data breach, they often say 'only email addresses and passwords were exposed' as if to minimize the damage. Why can this combination of data be more dangerous than it sounds? →

(A) Anger and outrage are high-engagement emotions — they drive more comments, shares, and time spent on the platform than positive content. The algorithm optimizes for engagement metrics, not user well-being

(B) The online disinhibition effect — screens create psychological distance, making people feel anonymous and detached from consequences

(C) Public Wi-Fi networks are often unencrypted, meaning a hacker on the same network could intercept Omar's login credentials using a 'man-in-the-middle' attack — capturing his username and password as they travel from his device to the email server

(D) Security questions are backup authentication used for password recovery. They are weak because the answers are often publicly available (social media, public records, genealogy sites) or guessable, and unlike passwords, you can't easily change facts like your mother's maiden name

(E) Because most people reuse passwords across multiple accounts — a leaked email-password pair from one site can be used to access banking, social media, school, and other accounts through credential stuffing attacks

15. Long-term Consequences

Circle the correct answer

141. Which of these activities contributes to your PASSIVE digital footprint (data collected about you without you directly choosing to share it)?

(A) Writing a product review on an online shopping site (B) Uploading a selfie to your social media profile (C) A website using cookies to track which pages you visit and how long you spend on each page (D) Sending a direct message to your friend on a messaging app

142. Two students debate whether location tracking on phones should be allowed:

Student A: 'Location tracking is great — it helps find lost phones, gives directions, and lets parents know kids are safe.'

Student B: 'Location tracking is dangerous — companies build detailed profiles of everywhere you go, and that data can be sold or hacked.'

Who has the stronger argument?

(A) Student A is right because safety always outweighs privacy concerns, based on the current recommendations from health professionals (B) Student B is right because location tracking should be completely banned, which is consistent with evidence-based health education (C) Neither is right because phones don't actually track your location, since this follows the recommended approach for young people (D) Both raise valid points — the answer depends on context. Location tracking has genuine utility, but the key issue is consent and control: users should be able to choose when, how, and by whom their location is tracked

143. What is an algorithm in the context of social media?

(A) The person at the company who manually chooses what you see, and this is the standard approach used in most cases (B) A set of rules and calculations that determines what content appears in your feed based on your past behavior, interests, and engagement patterns (C) A type of computer virus that spreads through social media, and this is the standard approach used in most cases (D) A settings menu where you select your favorite topics, which is why this approach is recommended by experts

144. A friend shares a meme that claims: 'Only 3% of the ocean has been explored — there could be anything down there!' The image shows a mysterious deep-sea creature. You research and find: the '3% explored' figure is outdated (modern estimates are 20-25% mapped), the image is an AI-generated creature, and the meme was created by a science fiction marketing account. However, the general point that much of the ocean is unexplored is true. How do you respond to your friend in a way

that corrects the misinformation without being dismissive?

(A) Tell your friend they should stop sharing misinformation and fact-check before posting, as this is what research and standard practice suggests, which is consistent with evidence-based health education (B) Acknowledge the valid underlying truth ('You're right that a lot of the ocean is still unexplored — it's actually about 75-80% unmapped, which is amazing'), then gently correct the specific errors ('I looked it up and the 3% number is outdated — we've actually mapped about 20-25%, and that creature image is AI-generated art from a sci-fi movie promotion. But the real deep-sea creatures are just as wild — check this out'), then share accurate but equally fascinating real information (C) Just ignore it — correcting friends about memes is socially awkward, making this the most widely accepted explanation, which aligns with the established guidelines for this age group (D) Report the meme to the platform for spreading false information, making this the most widely accepted explanation, according to the standard health and wellness practices

145. Rank these four 2FA methods from MOST secure to LEAST secure: (1) SMS text message codes, (2) Authenticator app (like Google Authenticator), (3) Physical security key (like a YubiKey), (4) Email-based codes.

(A) All four are equally secure because they all provide a second factor, according to the standard health and wellness practices (B) Email codes are most secure because email accounts have their own passwords, which aligns with the established guidelines for this age group (C) SMS is most secure because everyone has a phone and phone numbers can't be faked, since this follows the recommended approach for young people (D) Most to least secure: (3) Physical security key → (2) Authenticator app → (1) SMS text message → (4) Email-based codes. Security keys can't be phished or intercepted; authenticator apps generate codes locally; SMS can be intercepted via SIM swapping; email codes depend on your email account's security

146. What is a 'predatory journal' or 'predatory publisher'?

(A) A journal that charges readers a fee to access articles, and this is the standard approach used in most cases (B) A fraudulent academic publisher that charges authors fees to publish their work but provides little or no peer review, editorial oversight, or quality control — allowing unreliable or fabricated research to appear 'published' (C) A legitimate journal that publishes controversial research other journals won't accept, as this directly follows from the underlying principles (D) A wildlife conservation magazine, which is the most common explanation for this phenomenon

Write the answer

147. Sam accidentally sent an embarrassing photo to the wrong group chat. Now classmates are sharing it widely and adding mocking captions. Sam originally sent the photo voluntarily — does this mean it's Sam's fault and not cyberbullying?

Answer: _____

148. What is 'exclusion' as a form of cyberbullying?

Answer: _____

149. Liam gets 50 likes on a selfie and feels great. The next day he posts another selfie and only gets 12 likes. He feels disappointed and considers deleting the post. What psychological phenomenon explains why Liam's self-worth became tied to like counts?

Answer: _____

150. A company's privacy policy states: 'We may share anonymized and aggregated data with third-party partners for research and marketing purposes.' However, research shows that 'anonymized' data can often be re-identified. What is re-identification, and why does it make this policy statement misleading?

Answer: _____

Match each question to its answer

1. Compare how the concept of 'digital citizenship' might look different for a student in the United States, a student in the European Union, and a student in a country with heavy internet censorship. How do cultural, legal, and political contexts shape what digital citizenship means? →

2. Evaluate which verification method is MOST reliable when you receive a suspicious message claiming to be from your bank:

A) Reply to the suspicious email/text and ask if they are real

B) Call the phone number provided in the suspicious message

C) Look up your bank's official phone number independently and call them

D) Ask your friend who works at a different bank if the message seems real →

3. What is the 'social comparison trap' on social media? →

4. Explain why the phrase 'I have nothing to hide, so I don't need privacy' is a flawed argument. →

5. Which of the following is an example of cyberbullying? →

(A) The tendency to compare your everyday life to other people's carefully curated highlight reels, leading to feelings of inadequacy even though the comparison is unfair

(B) US: Strong free speech protections but weaker privacy laws (no COPPA equivalent for teens 13+); digital citizenship emphasizes individual responsibility. EU: Strong privacy rights (GDPR), right to be forgotten, content moderation requirements; digital

citizenship emphasizes data rights. Censored country: Limited access to global platforms, government surveillance, VPN use may be illegal; digital citizenship includes navigating censorship and understanding state control of information. The CORE principles (safety, privacy, critical thinking) are universal, but their APPLICATION is deeply shaped by local legal, cultural, and political realities

(C) Creating a fake social media account to post embarrassing things about a classmate

(D) C Look up your bank's official phone number independently (from your bank card, official website, or previous statements) and call them directly. This is the only method that guarantees you're communicating with the actual bank and not the scammer

(E) Privacy isn't about hiding wrongdoing — it's a fundamental right that protects against discrimination, manipulation, power imbalances, and the chilling effect on free expression. Everyone has information they rightfully keep private

16. Long-term Consequences

Circle the correct answer

151. What does the acronym 'PII' stand for, and why is it important in digital safety?

(A) PII stands for Private Internal Information and only applies to government employees, making this the most widely accepted explanation (B) PII stands for Personal Internet Identity and refers to your username on social media, and this has been consistently demonstrated in practice (C) PII stands for Personally Identifiable Information — data that can identify a specific person, like full name, address, phone number, Social Security number, or email. Protecting PII prevents identity theft, stalking, and unauthorized account access (D) PII stands for Public Internet Index and measures how popular you are online, making this the most widely accepted explanation

152. What is 'multi-factor authentication' and how is it different from two-factor authentication?

(A) Multi-factor authentication (MFA) uses two or more different authentication factors — it is the general term, while two-factor authentication (2FA) is the specific case of using exactly two factors. Three-factor authentication would be MFA using three different factors (e.g., password + phone code + fingerprint) (B) Multi-factor means using many passwords at once, while two-factor uses only two passwords, as this directly follows from the underlying principles (C) MFA is for businesses only and 2FA is for personal accounts only, as this is what research and standard practice suggests (D) There is no difference — MFA and 2FA are two abbreviations for the same exact thing, as this directly follows from the underlying principles

153. What is the 'paradox of tolerance' as it applies to online spaces?

(A) The theory that spending more time online makes people less patient in real life, which is the most common explanation for this phenomenon (B) The paradox of tolerance states that unlimited tolerance ultimately leads to the disappearance of tolerance — if a platform tolerates all speech including hate speech and harassment, the hateful voices drive away marginalized users, creating a less tolerant space. Some content moderation is necessary to maintain an inclusive environment (C) The idea that tolerant people are actually intolerant of others' beliefs, making this the most widely accepted explanation (D) A setting on social media that makes you more tolerant of different opinions, which is why this approach is recommended by experts

154. What is a 'brute force attack' and how does password length protect against it?

(A) Password length doesn't matter for brute force attacks because they start with the longest passwords first (B) Brute force attacks only work on passwords that contain the word 'brute', and this is the standard approach used in most cases (C) A brute force attack uses physical force to break into the computer hardware, and this is the standard approach used in most cases (D) A brute force attack tries every possible password combination until finding the correct one. Longer passwords protect against it because each additional character multiplies the total number of combinations — a 12-character password has trillions of times more combinations than a 6-character password, making brute force impractical

155. Two messaging apps have different approaches to privacy:

App A: Free, stores messages on company servers, scans content for targeted ads, shares data with advertisers. 2 billion users.

App B: Free and open-source, end-to-end encrypted, stores no messages on servers, funded by donations. 40 million users.

Why might someone choose App A despite its weaker privacy?

(A) Because App A is better technology in every way, which is consistent with evidence-based health education (B) Because App B's encryption makes messages unreadable, according to the standard health and wellness practices (C) Network effects — if all your friends and family use App A, switching to App B means losing communication access. The value of a messaging app depends on who else uses it, creating a lock-in effect that outweighs privacy concerns for many people (D) Because people who use App A don't care about privacy at all, based on the current recommendations from health professionals

156. A stranger in an online game tells you they work for the game company and can give you free premium currency if you share your login details. How should you respond?

(A) Never share login details — real game company employees would never ask for your password in-game. This is a social engineering scam. Report the user to the

game's moderation team and block them (B) Give them your username but not your password — they only need the username to add currency (C) Ask them to prove they're a real employee by giving you their employee ID number first (D) Share your password because employees have special tools to add currency to your account

Write the answer

157. Identify the propaganda technique used in each statement:

A: 'Every real American supports this policy.'

B: 'Dr. Smith, a famous heart surgeon, says this energy drink is the healthiest option.'

C: 'This politician is just like Hitler.'

Answer: _____

158. Jaylen receives a direct message from an account claiming to be a talent scout: 'I saw your basketball highlights on TikTok! I work with Nike and want to sponsor you. Send me your full name, school address, and parent's phone number so I can mail a contract. Don't tell anyone yet — this is an exclusive offer!' Apply your digital citizenship knowledge to identify every red flag in this message.

Answer: _____

159. Marcus discovers that his younger sister (age 9) has been chatting with someone online who claims to be a 12-year-old girl but has been asking increasingly personal questions about the family — where they live, when parents are home, and what the house looks like. Marcus recognizes this as suspicious. What should he do, and in what order?

Answer: _____

160. A 13-year-old influencer with 100,000 followers promotes a weight-loss supplement. The post includes '#ad' in small text at the end. Analyze this situation from child safety, advertising ethics, misinformation, and digital wellness perspectives.

Answer: _____

Match each question to its answer

1. A study finds that teens who spend 3+ hours daily on social media have twice the risk of depression symptoms compared to those who spend less than 1 hour. A news headline reads: 'Social Media CAUSES Teen Depression!' Evaluate whether the headline accurately represents the study's findings. →

2. Research shows that social media affects boys and girls differently. For girls, negative effects peak around ages 11-13. For boys, the peak is around ages 14-15. Why might the timing differ, and what implications does this have for digital wellness education? →

3. Explain why digital citizenship skills become MORE important, not less, as technology advances. →
4. A pop-up appears while you're browsing: 'WARNING! Your computer is infected with 5 viruses! Call 1-800-555-HELP immediately or your data will be destroyed!' What type of scam is this? →
5. Why do social media platforms use 'infinite scroll' instead of pagination (numbered pages)? →

(A) The headline is misleading — the study shows a correlation (association) between social media use and depression, not causation. Depressed teens might use more social media as a coping mechanism, or a third factor (like loneliness) could cause both. Correlation does not prove causation

(B) This is a 'tech support scam' or 'scareware' — a fake warning designed to frighten you into calling a number where scammers will ask for remote access to your computer or payment for unnecessary 'repairs.' Real antivirus software never uses browser pop-ups to report infections

(C) As technology becomes more powerful and integrated into daily life, the stakes increase: AI makes misinformation more convincing, IoT expands surveillance, social media's psychological effects deepen, and digital decisions have more real-world consequences. Skills that protect against manipulation, privacy invasion, and online harm must evolve alongside the technology that creates these threats

(D) Infinite scroll removes natural stopping points, making it harder for users to decide to stop browsing — it exploits the brain's tendency to keep consuming when there's no clear endpoint

(E) The timing aligns with puberty onset (earlier for girls) when self-image, social comparison, and peer validation become most important. This means digital wellness education needs to be age-and-gender-aware, reaching girls before middle school and boys during early high school

Riddle & Joke Break

Guess the answer, then check the key!

161. I changed my password to "incorrect" so my computer always tells me when I forget it: "Your password is incorrect."

162. My digital footprint is so big, even Bigfoot is impressed.

163. Phishing emails are like bad fishing trips -- they throw out a lot of bait, but you should never bite.

164. The firewall applied for a job in security. It said, "I've been blocking threats for years -- it's kind of my whole thing."

165. My privacy settings and I have a close relationship -- I keep them tight.

166. Two-factor authentication walks into a bar. The bouncer says, "ID please." 2FA says, "Here's my ID AND a code from my phone." The bouncer is impressed.

Answer Key

1. C — The trail of data and information you leave behind whenever you use the internet — including posts, searches, photos, comments, and account activity
2. B — An active digital footprint is data you intentionally share (like posting a photo or writing a comment), while a passive digital footprint is data collected about you without your direct action (like websites tracking which pages you visit)
3. C — No — even though Maya deleted her post, the photo may still exist in the app's backup servers, in friends' screenshots, in cached copies on search engines, or if someone shared or saved it before deletion
4. C — Your home address, school name, phone number, or full birthday (including the year you were born)
5. D — The username reveals his real name (Liam Smith), birth year (2014), and city (Chicago), and using it across multiple platforms lets anyone connect all his accounts and build a detailed profile of him
6. B — The overall picture of who you are online — built from your usernames, profiles, posts, comments, photos, likes, and how you interact with others across all platforms
7. Sharing her science fair project online, writing encouraging comments on friends' posts, and joining a student volunteer group's page
8. Jake should consider how the classmate would feel seeing that video online, that the video could spread beyond his friends and become permanent, that it could be considered cyberbullying, and that it could damage both the classmate's and Jake's own digital reputation
9. They want to see if your online behavior matches the responsible, respectful person you claim to be in your application — your digital footprint reveals character, judgment, and how you treat others
10. The anonymous account, because commenting on public news articles with her real name and photo could expose her identity to strangers and connect her opinions to her real-world identity permanently

Matching (Digital Identity and Footprint): 1→B, 2→E, 3→C, 4→A, 5→D

11. C — A strong password is long (at least 12 characters), uses a mix of uppercase letters, lowercase letters, numbers, and symbols, and does not contain easily guessable information like your name, birthday, or common words
12. B — If one account is hacked or leaked in a data breach, the attacker can use that same password to access ALL your other accounts — email, gaming, social media, and everything else
13. A — C) 'My-Cat-Loves-Tuna-Sandwiches!' — it is the longest (32 characters), uses a passphrase format that is easy to remember but hard to crack, and includes uppercase, lowercase, hyphens, and a symbol
14. D — Two-factor authentication requires two different types of proof to log in — something you know (your password) plus something you have (like a code sent to your phone) — so even if someone steals your password, they still cannot access your account without the second factor
15. D — Zoe should not share her password — even with a trusted friend. Sharing passwords gives another person access to personal messages, payment information, and the ability to make purchases or changes under Zoe's name
16. B — A data breach is when hackers break into a company's database and steal user information — including usernames, passwords, email addresses, and sometimes credit card numbers. Your data could be exposed even if you did nothing wrong, because the company failed to protect it
17. A password manager is a secure application that generates, stores, and auto-fills unique strong passwords for all your accounts. You only need to remember one master password, and the manager handles the rest — solving the impossible task of remembering dozens of unique passwords
18. Do NOT click the link — this is a phishing attempt. Legitimate companies never ask you to verify your password by clicking an email link. Marcus should go directly to Roblox.com by typing the address himself and check his account status there, or ask a parent for help
19. Authentication is like showing your student ID to enter the school building — proving you are who you claim to be. Authorization is like your class schedule determining which rooms you can enter — your ID gets you in the building, but you're only allowed in certain classrooms, not the principal's office or teacher's lounge
20. Social engineering is when someone manipulates people psychologically to trick them into revealing passwords, personal information, or access — exploiting

human trust and emotions rather than hacking computer systems directly
Matching (Password Security and Account Protection): 1→A, 2→B, 3→E, 4→C, 5→D

21. C — A type of online scam where attackers disguise themselves as trustworthy organizations (banks, schools, popular apps) to trick people into revealing personal information like passwords, credit card numbers, or account credentials
22. C — Red flags include: (1) urgent language pressuring immediate action ('Your account will be closed in 24 hours!'), (2) a sender email address that doesn't match the claimed organization (e.g., 'support@amaz0n-security.com' instead of '@amazon.com'), and (3) requests for sensitive information like passwords or credit card numbers via email
23. D — This is likely phishing. Red flags: the sender domain 'school-portal-update.net' doesn't match the school's actual domain, it creates urgency with a deadline and a threat of losing access, and schools typically communicate password updates through official channels — not via email links. You should verify by contacting the school IT department directly
24. C — Smishing is phishing conducted through SMS text messages instead of email. Attackers send texts that appear to be from banks, delivery services, or government agencies, containing links to fake websites designed to steal personal information
25. C — This is a 'tech support scam' or 'scareware' — a fake warning designed to frighten you into calling a number where scammers will ask for remote access to your computer or payment for unnecessary 'repairs.' Real antivirus software never uses browser pop-ups to report infections
26. C — A fake website is a copy of a legitimate site designed to steal login credentials or payment information. You can spot fakes by checking: the URL carefully (amazom.com vs amazon.com), looking for HTTPS, examining the domain spelling, checking for poor design quality, and verifying through a search engine rather than clicking links
27. This is a classic 'free prize' scam. The real goal is to collect your credit card information — the \$1.99 charge is a pretext to get your card details, which will then be used for unauthorized charges. Legitimate companies don't give away expensive products to random social media users
28. Spear phishing targets a specific individual using personal information gathered about them (from social media, school websites, or data breaches) to create a highly convincing personalized message. It's more dangerous because the message feels real — it may reference your name, school, friends, or recent activities

29. Never share login details — real game company employees would never ask for your password in-game. This is a social engineering scam. Report the user to the game's moderation team and block them
30. The grandparent scam involves a caller pretending to be a grandchild in trouble (arrested, in an accident, stranded abroad), urgently needing money wired or gift cards purchased. It exploits the love and panic grandparents feel for their grandchildren, causing them to act emotionally without verifying the story
Matching (Recognizing Online Scams and Phishing): 1→D, 2→C, 3→E, 4→A, 5→B
31. D — Using digital devices to repeatedly and intentionally harass, threaten, or humiliate someone
32. B — Creating a fake social media account to post embarrassing things about a classmate
33. D — Someone who speaks up or takes action to support a person being bullied
34. B — It can happen 24/7, reach a large audience instantly, and leave a permanent digital record
35. D — Harassment — repeated hostile messages targeting a specific person
36. B — Save screenshots as evidence, then report the fake account to Instagram and tell a trusted adult
37. Even a single message can be cyberbullying if it's severe enough — threats or attempts to isolate someone cross the line regardless of frequency
38. A = Outing/doxing, B = Exclusion, C = Cyberstalking/threats
39. Program B — it builds student skills and provides safe reporting, creating lasting behavioral change
40. Send a private supportive message to the target, report the comments to TikTok, and tell a trusted adult
Matching (Cyberbullying Prevention and Response): 1→B, 2→D, 3→E, 4→A, 5→C
41. A — Any data that can be used to identify a specific individual, such as full name, address, phone number, or Social Security number
42. D — A legal document that explains how a company collects, uses, stores, and shares your personal data
43. D — They collect and monetize user data through targeted advertising — the user's attention and data are the product being sold
44. D — Collection is gathering information directly from users; sharing is providing

that collected data to third parties like advertisers, partners, or data brokers

45. C — The permissions far exceed what a flashlight needs — the app is likely collecting unnecessary data and should not be trusted
46. B — Provide only what's necessary: a username (not real name), parent's email for account verification. Avoid sharing school name, home address, and phone number — these are unnecessary for gaming and create safety risks
47. She has broadcast that her home is unoccupied for a specific duration, shared her exact current location, and created a pattern that could be used for burglary or stalking
48. Re-identification is the process of matching 'anonymous' data back to specific individuals by combining multiple data points — making the promise of anonymity false because datasets that seem anonymous can be cross-referenced to identify people
49. GDPR provides stronger protection — it covers 14-year-olds (COPPA stops at 13), includes the right to erasure ('right to be forgotten'), and applies to all companies serving EU residents regardless of where the company is based
50. Both raise valid points — the answer depends on context. Location tracking has genuine utility, but the key issue is consent and control: users should be able to choose when, how, and by whom their location is tracked
Matching (Privacy and Personal Information): 1→E, 2→D, 3→C, 4→B, 5→A
51. B — A set of rules and calculations that determines what content appears in your feed based on your past behavior, interests, and engagement patterns
52. B — When algorithms show you only content that matches your existing beliefs and interests, isolating you from diverse perspectives
53. A — Infinite scroll removes natural stopping points, making it harder for users to decide to stop browsing — it exploits the brain's tendency to keep consuming when there's no clear endpoint
54. B — The tendency to compare your everyday life to other people's carefully curated highlight reels, leading to feelings of inadequacy even though the comparison is unfair
55. D — A variable reward loop — unpredictable notifications create dopamine spikes similar to slot machines, and the anxiety between checks resembles withdrawal from intermittent reinforcement
56. B — Carlos is investing significant time maintaining superficial connections far beyond his meaningful relationship capacity. The 1,185 followers he doesn't

interact with provide social validation metrics but not genuine connection — he's optimizing for numbers rather than relationship quality

- 57. Compulsively consuming negative or distressing news content online, even though it worsens your mood and anxiety
- 58. Anger and outrage are high-engagement emotions — they drive more comments, shares, and time spent on the platform than positive content. The algorithm optimizes for engagement metrics, not user well-being
- 59. Social media posts are curated performances, not authentic documentation — the gap between posted content and lived reality means that comparing your life to others' posts is comparing your full experience to their edited highlight reel
- 60. Not necessarily — chronological feeds solve filter bubbles but can increase FOMO (fear of missing out) since you might miss important posts, and the platform may still use other persuasive design techniques like infinite scroll, notifications, and like counts

Matching (Social Media Literacy and Digital Wellness): 1→E, 2→B, 3→C, 4→D, 5→A

- 61. A — Misinformation is false information shared without intent to deceive (the sharer believes it's true); disinformation is false information deliberately created and spread to mislead people
- 62. A — Confirmation bias is the tendency to seek, interpret, and remember information that confirms existing beliefs while ignoring contradictory evidence — it makes people more likely to believe and share misinformation that aligns with what they already think
- 63. B — Instead of evaluating a website by reading its content deeply, you open new tabs to search what OTHER sources say about the site, its author, and its claims — reading 'laterally' across multiple sources rather than 'vertically' within one source
- 64. B — Misinformation is often more novel, emotionally provocative, and surprising than facts — it triggers stronger emotional reactions that drive sharing. Algorithms amplify engaging content regardless of accuracy, and the human brain processes emotional content before analytical evaluation
- 65. D — Stop — don't share yet. Investigate — search for 'Journal of Health Research' (is it a reputable peer-reviewed journal or a predatory journal?). Find better coverage — search the claim on fact-checking sites and legitimate health news. Trace — find the original study to check if it actually says what the post claims (likely it found a correlation, not that chocolate 'prevents' cancer)
- 66. A — Open new tabs to: (1) search the website name — check if it's a known

misinformation site, (2) search the specific claim on local news outlets and government health sites, (3) check if any established news organizations are reporting the same story, (4) look for official water quality reports from local authorities. If only this one unknown site reports it, the claim is likely false

67. AI-generated synthetic media that convincingly replaces a person's likeness or voice in video or audio — making it appear that someone said or did something they never actually did
68. No — popularity metrics (views, likes, comments) measure engagement, not accuracy. Viral content is often sensational or emotionally triggering, which drives views regardless of truthfulness. Bots and coordinated campaigns can also artificially inflate metrics
69. A = Bandwagon (everyone's doing it, join in), B = False authority (expert in one field endorsing something outside their expertise), C = Reductio ad Hitlerum / false analogy (comparing to an extreme to discredit)
70. The illusory truth effect is the psychological phenomenon where repeated exposure to a claim makes it feel more true, regardless of its actual accuracy. On social media, false claims that circulate repeatedly become more believable simply because people have seen them multiple times
Matching (Critical Thinking and Misinformation Online): 1→D, 2→C, 3→E, 4→B, 5→A
71. C — The responsible, ethical, and informed use of technology — encompassing online safety, privacy awareness, respectful communication, critical information evaluation, and understanding your rights and responsibilities in digital spaces
72. A — Digital identity and footprint, password security and account protection, online safety (scams, phishing, cyberbullying), privacy and personal information, and media/information literacy (misinformation, social media awareness)
73. C — As technology becomes more powerful and integrated into daily life, the stakes increase: AI makes misinformation more convincing, IoT expands surveillance, social media's psychological effects deepen, and digital decisions have more real-world consequences. Skills that protect against manipulation, privacy invasion, and online harm must evolve alongside the technology that creates these threats
74. C — They're deeply interconnected: your digital footprint determines what information is available about you (privacy exposure), which cyberbullies can exploit to target you more effectively. Example: a student shares their school name in a gaming profile (footprint), which reveals their location (privacy gap), which a cyberbully uses to make real-world threats ('I know where you go to

school'). Conversely, cyberbullying creates a negative digital footprint for the target through spread of harmful content

75. C — Red flags: (1) Unsolicited contact from a stranger requesting PII (full name, school address, parent's phone). (2) Urgency and exclusivity pressure ('don't tell anyone yet'). (3) Legitimate companies don't recruit minors through DMs. (4) Real sponsorships go through official channels with parental involvement from the start. (5) Requesting physical addresses via DM is a safety concern. (6) 'Don't tell anyone' is the #1 grooming tactic — isolating the target from trusted adults. (7) No verifiable company contact information provided
76. D — Privacy analysis: Complete footprint deletion is technically impossible — data exists on thousands of servers, in backups, screenshots, and data broker databases. Misinformation analysis: The before/after could be easily faked or show cached vs non-cached results; the claim is extraordinary and requires extraordinary evidence. Persuasive design analysis: The viral spread, positive comments (possibly bot-generated), and too-good-to-be-true promise follow typical scam patterns. The app likely harvests MORE data rather than deleting existing data
77. Algorithms maximize engagement by showing content that triggers strong reactions. Filter bubbles limit exposure to diverse viewpoints, creating echo chambers. These echo chambers become fertile ground for misinformation because: users only see confirming information (confirmation bias), the illusory truth effect makes repeated false claims feel true, and there are no counter-perspectives to challenge false narratives
78. Privacy: 24/7 monitoring on a mandatory device invades student privacy, especially during personal time — it captures non-school activity in students' homes. Safety benefits: monitoring can identify cyberbullying, self-harm indicators, and inappropriate content access. Potential harms: chilling effect on legitimate research (students avoid searching sensitive health/identity topics), disproportionate impact on students exploring LGBTQ+ identity or mental health in unsupportive homes, false positives from 'concerning' keywords in legitimate schoolwork, and the surveillance teaches compliance rather than self-regulation
79. Digital footprint: The teacher now has a false narrative permanently associated with their name online. Misinformation: A decontextualized clip created a false impression — the 15 seconds was technically real but deeply misleading without the full context. Mob mentality: 10,000 signatures demonstrate how quickly online outrage spreads before verification; social proof encouraged signing without investigation. Real-world consequences: A teacher acting heroically could lose their career based on a misleading clip, demonstrating how digital actions have devastating real-world impacts

80. The paradox of tolerance states that unlimited tolerance ultimately leads to the disappearance of tolerance — if a platform tolerates all speech including hate speech and harassment, the hateful voices drive away marginalized users, creating a less tolerant space. Some content moderation is necessary to maintain an inclusive environment

Matching (Master Digital Citizen Capstone): 1→D, 2→E, 3→A, 4→B, 5→C

81. D — Stop, drop, and roll

82. C — At least once a month

83. C — Crawl low under the smoke

84. B — 911

85. D — Smoke alarm

86. C — A home fire escape plan

87. To check if fire or heat is on the other side

88. One exit may be blocked by fire or smoke

89. Once you escape, never go back inside a burning building

90. A closed door slows the spread of fire and smoke

Matching (Safety & Preparedness): 1→A, 2→D, 3→C, 4→E, 5→B

91. B — Cool the burn under cool running water for at least 10 minutes

92. D — Cardiopulmonary resuscitation

93. D — A clean cloth or bandage

94. C — 911

95. B — A collection of supplies used to treat minor injuries and stabilize serious ones until help arrives

96. C — The person is lying on their side with their top leg bent for stability

97. To remove dirt and bacteria that could cause infection

98. To protect both you and the injured person from bloodborne infections

99. The object may be controlling bleeding, and removing it could cause more damage

100. Moving them could damage the spinal cord and cause permanent paralysis

Matching (Safety & Preparedness): 1→C, 2→E, 3→A, 4→D, 5→B

101. A — Drop, cover, and hold on under a sturdy piece of furniture
102. C — A basement or an interior room on the lowest floor, away from windows
103. A — A collection of essential supplies to survive for at least 72 hours after a disaster
104. B — One gallon per person per day
105. D — Conditions are favorable for tornadoes to develop — be prepared
106. A — Earthquake
107. Phone lines may be overwhelmed and family members may be separated — a plan ensures everyone knows how to reconnect
108. Just 6 inches of moving water can knock you down, and 2 feet can float a car
109. Originals may be destroyed in a disaster, and you may need identification, insurance, and medical records
110. An undersea earthquake displaces a massive volume of water, creating waves that travel across the ocean
Matching (Safety & Preparedness): 1→A, 2→C, 3→E, 4→B, 5→D
111. A — A long, unique combination of letters, numbers, and symbols that is hard to guess
112. B — A scam where someone pretends to be a trusted source to trick you into sharing personal information
113. A — A trusted adult, like a parent or teacher
114. B — Using technology to harass, threaten, embarrass, or target another person
115. A — Full name, address, school name, phone number, and passwords
116. A — The website uses encryption (HTTPS) to protect data sent between you and the site
117. If one account is hacked, the attacker cannot access all your other accounts
118. Once posted, content can be screenshot, shared, and may never be fully deleted — it could affect your reputation forever
119. They create urgency or fear, mimic trusted brands, and use official-looking logos and language
120. It tells strangers exactly where you are in real time, which could be used to track or find you

Matching (Safety & Preparedness): 1→A, 2→C, 3→B, 4→D, 5→E

- 121. C — The trail of data and information you leave behind whenever you use the internet — including posts, searches, photos, comments, and account activity
- 122. A — No — even though Maya deleted her post, the photo may still exist in the app's backup servers, in friends' screenshots, in cached copies on search engines, or if someone shared or saved it before deletion
- 123. B — Your home address, school name, phone number, or full birthday (including the year you were born)
- 124. A — The username reveals his real name (Liam Smith), birth year (2014), and city (Chicago), and using it across multiple platforms lets anyone connect all his accounts and build a detailed profile of him
- 125. C — The overall picture of who you are online — built from your usernames, profiles, posts, comments, photos, likes, and how you interact with others across all platforms
- 126. A — Sharing her science fair project online, writing encouraging comments on friends' posts, and joining a student volunteer group's page
- 127. Jake should consider how the classmate would feel seeing that video online, that the video could spread beyond his friends and become permanent, that it could be considered cyberbullying, and that it could damage both the classmate's and Jake's own digital reputation
- 128. They want to see if your online behavior matches the responsible, respectful person you claim to be in your application — your digital footprint reveals character, judgment, and how you treat others
- 129. The anonymous account, because commenting on public news articles with her real name and photo could expose her identity to strangers and connect her opinions to her real-world identity permanently
- 130. Small text files that websites store on your device to remember information about you — like login status, preferences, items in a shopping cart, and your browsing activity on that site

Matching (Long-term Consequences): 1→B, 2→E, 3→A, 4→C, 5→D

- 131. B — Do not share it — tell your friend that spreading altered images of someone without their consent is hurtful and could be considered cyberbullying, and suggest they delete it too
- 132. D — These questions match common security questions used for account recovery. The quiz is likely designed to harvest answers to security questions —

with your email, birthday, mother's maiden name, and childhood street, an attacker could reset passwords on many of your accounts

133. C — Zoe should not share her password — even with a trusted friend. Sharing passwords gives another person access to personal messages, payment information, and the ability to make purchases or changes under Zoe's name
134. B — C) 'My-Cat-Loves-Tuna-Sandwiches!' — it is the longest (32 characters), uses a passphrase format that is easy to remember but hard to crack, and includes uppercase, lowercase, hyphens, and a symbol
135. B — The scammers used information from Rachel's public Instagram posts to make the phishing message seem legitimate — mentioning Hawaii matches her actual location, making the 'unusual activity' warning feel real and urgent. This is spear phishing using publicly available social media data
136. D — Any data that can be used to identify a specific individual, such as full name, address, phone number, or Social Security number
137. Free piracy sites are loaded with security risks: malicious ads that install malware, fake 'video player' downloads that are actually viruses, pop-ups leading to phishing sites, cryptocurrency miners running in your browser, and exposure to inappropriate or shocking content in ads
138. No — popularity metrics (views, likes, comments) measure engagement, not accuracy. Viral content is often sensational or emotionally triggering, which drives views regardless of truthfulness. Bots and coordinated campaigns can also artificially inflate metrics
139. A legal document that explains how a company collects, uses, stores, and shares your personal data
140. Publicly revealing someone's private personal information online without their consent
Matching (Long-term Consequences): 1→C, 2→A, 3→D, 4→B, 5→E
141. C — A website using cookies to track which pages you visit and how long you spend on each page
142. D — Both raise valid points — the answer depends on context. Location tracking has genuine utility, but the key issue is consent and control: users should be able to choose when, how, and by whom their location is tracked
143. B — A set of rules and calculations that determines what content appears in your feed based on your past behavior, interests, and engagement patterns
144. B — Acknowledge the valid underlying truth ('You're right that a lot of the ocean

is still unexplored — it's actually about 75-80% unmapped, which is amazing'), then gently correct the specific errors ('I looked it up and the 3% number is outdated — we've actually mapped about 20-25%, and that creature image is AI-generated art from a sci-fi movie promotion. But the real deep-sea creatures are just as wild — check this out'), then share accurate but equally fascinating real information

145. D — Most to least secure: (3) Physical security key → (2) Authenticator app → (1) SMS text message → (4) Email-based codes. Security keys can't be phished or intercepted; authenticator apps generate codes locally; SMS can be intercepted via SIM swapping; email codes depend on your email account's security
146. B — A fraudulent academic publisher that charges authors fees to publish their work but provides little or no peer review, editorial oversight, or quality control — allowing unreliable or fabricated research to appear 'published'
147. No — sharing the photo with mocking intent is cyberbullying regardless of how the photo was originally shared. Sending something to one group doesn't consent to it being spread everywhere
148. Deliberately and repeatedly leaving someone out of online groups, chats, or gaming sessions
149. External validation dependency — Liam has begun measuring his self-worth through social approval metrics rather than internal self-assessment. The variable like counts create a conditioning pattern where self-esteem fluctuates with each post's performance
150. Re-identification is the process of matching 'anonymous' data back to specific individuals by combining multiple data points — making the promise of anonymity false because datasets that seem anonymous can be cross-referenced to identify people
Matching (Long-term Consequences): 1→B, 2→D, 3→A, 4→E, 5→C
151. C — PII stands for Personally Identifiable Information — data that can identify a specific person, like full name, address, phone number, Social Security number, or email. Protecting PII prevents identity theft, stalking, and unauthorized account access
152. A — Multi-factor authentication (MFA) uses two or more different authentication factors — it is the general term, while two-factor authentication (2FA) is the specific case of using exactly two factors. Three-factor authentication would be MFA using three different factors (e.g., password + phone code + fingerprint)
153. B — The paradox of tolerance states that unlimited tolerance ultimately leads to the disappearance of tolerance — if a platform tolerates all speech including

hate speech and harassment, the hateful voices drive away marginalized users, creating a less tolerant space. Some content moderation is necessary to maintain an inclusive environment

154. D — A brute force attack tries every possible password combination until finding the correct one. Longer passwords protect against it because each additional character multiplies the total number of combinations — a 12-character password has trillions of times more combinations than a 6-character password, making brute force impractical
155. C — Network effects — if all your friends and family use App A, switching to App B means losing communication access. The value of a messaging app depends on who else uses it, creating a lock-in effect that outweighs privacy concerns for many people
156. A — Never share login details — real game company employees would never ask for your password in-game. This is a social engineering scam. Report the user to the game's moderation team and block them
157. A = Bandwagon (everyone's doing it, join in), B = False authority (expert in one field endorsing something outside their expertise), C = Reductio ad Hitlerum / false analogy (comparing to an extreme to discredit)
158. Red flags: (1) Unsolicited contact from a stranger requesting PII (full name, school address, parent's phone). (2) Urgency and exclusivity pressure ('don't tell anyone yet'). (3) Legitimate companies don't recruit minors through DMs. (4) Real sponsorships go through official channels with parental involvement from the start. (5) Requesting physical addresses via DM is a safety concern. (6) 'Don't tell anyone' is the #1 grooming tactic — isolating the target from trusted adults. (7) No verifiable company contact information provided
159. Immediate actions in order: (1) Don't alert the suspicious person (don't tip them off). (2) Save/screenshot the conversation as evidence. (3) Tell a parent/guardian IMMEDIATELY — this is a potential predator situation that requires adult intervention. (4) The parent should report to the platform, contact local police (many have cyber units), and file a report with the FBI's IC3 or NCMEC CyberTipline. (5) Have an age-appropriate conversation with the sister about online stranger danger without blaming her
160. Child safety: A minor promoting health products to a young audience creates pressure on developing body images. Advertising ethics: '#ad' disclosure is technically present but minimized, and the FTC requires clear/prominent disclosure. Misinformation: Weight-loss supplements are largely unregulated and the influencer likely lacks scientific knowledge to evaluate health claims. Digital wellness: Social comparison from a peer-age influencer promoting appearance

modification is more psychologically impactful than the same message from an adult. Combined: this is a minor being commercially exploited to sell unregulated health products to other minors

Matching (Long-term Consequences): 1→A, 2→E, 3→C, 4→B, 5→D

161. I changed my password to "incorrect" so my computer always tells me when I forget it: "Your password is incorrect."
162. My digital footprint is so big, even Bigfoot is impressed.
163. Phishing emails are like bad fishing trips -- they throw out a lot of bait, but you should never bite.
164. The firewall applied for a job in security. It said, "I've been blocking threats for years -- it's kind of my whole thing."
165. My privacy settings and I have a close relationship -- I keep them tight.
166. Two-factor authentication walks into a bar. The bouncer says, "ID please." 2FA says, "Here's my ID AND a code from my phone." The bouncer is impressed.

Spark & Anvil is a 501(c)(3) public charity. Apps + books are free forever.