Family Cybersecurity Quiz

Quiz · Test Your Household's Collective Cyber-Awareness.

Your defence is only as strong as your most exposed family member. Test your knowledge across kids, teens, elderly relatives, and the family-wide systems that protect everyone.

Instructions

10 multiple-choice questions. Pick the BEST answer for each. Don't peek at the answer key on the next page. Score yourself at the end. There's no time limit, but most people finish in 5-7 minutes.

Questions

Q1. What's a family verify-word system?

A. A shared password for all family accounts

B. A code word each family member knows to authenticate urgent money requests — defends against AI-voice and impersonation scams

C. A list of approved websites for kids

D. A weekly meeting agenda

Q2. If your child or teen tells you they've encountered something inappropriate or scary online, the best response is:

A. Punish them for whatever they did to encounter it

B. Listen without immediate judgement — the goal is for them to report things to you

C. Take their devices away as the first step

D. Tell them to figure it out themselves

Q3. When should kids' credit be frozen?

A. Only after they turn 18

B. As young as possible — child identity theft is common, and a frozen file with no credit history protects them

C. Only if you suspect fraud

D. Never — it limits their future options

Q4. A grandchild calls in tears asking for emergency bail money and begging you not to tell their parents. What should you do?

A. Wire the money immediately

B. Hang up and call the grandchild's parents directly to verify

C. Send via gift cards as instructed

D. Drive to the courthouse

Q5. What's the most effective way to protect elderly parents from common scams?

A. Take their phones away

B. Set up identity protection, fraud alerts on accounts, agreed verify-words, and have ongoing scam-pattern conversations

C. Buy them a new device

D. Tell them to stop using technology

Q6. Should family members share passwords with each other?

A. Yes — for convenience, share via text

B. Only via secure password-manager sharing for legitimately shared accounts; never via insecure channels

C. Always — there's no risk

D. Never — even shared accounts should have separate logins

Q7. Which of these is the highest-risk online platform for kids 10-13?

A. Public messaging apps where strangers can DM them

B. School-managed Google Classroom

C. Family group chats

D. Curated kids' streaming services

Q8. What's the best parental-control approach for teens (14-17)?

A. Monitor everything secretly

B. Combine reasonable controls (screen time, app limits) with ongoing conversations and trust-building

C. Give them complete freedom

D. Use only physical lockboxes for devices

Q9. If a teen sends a sensitive image and is then threatened (sextortion), the FIRST thing to do is:

A. Ignore the threat

B. Pay the demand

C. Stop responding to the threat, document evidence, tell a trusted adult, report to the platform AND law enforcement (FBI for minors)

D. Delete all of the teen's accounts

Q10. How often should the family discuss cybersecurity together?

A. Never — it's boring

B. At least quarterly check-ins, and after any scam attempt or news event the family should know about

C. Only when something goes wrong

D. Only when buying a new device

Answer Key

Don't peek before completing the quiz. Read explanations even for answers you got right — they reinforce the why.

Q1: B — Verify-word system defends against AI voice cloning and family-emergency scams. If a 'family member' calls in distress, they need to say the word.

Q2: B — Reporting must be safe. Punishing the messenger means future scary things won't be reported — and damage will be worse.

Q3: B — Child identity theft hits ~1M kids/year. A frozen file with no credit history is the strongest defence. Free for minors.

Q4: B — Grandchild emergency scam — often AI voice cloning. Always verify via the actual family member's known number.

Q5: B — Elderly relatives need layered defences. Paid IDP often makes sense for them. Ongoing conversations matter as much as tech.

Q6: B — Use the password manager's secure sharing for joint accounts (Netflix, etc.). Never share via insecure channels.

Q7: A — Apps with stranger-DM access are the highest predator risk for kids. Locked-down apps are far safer.

Q8: B — Teens need autonomy paired with reasonable structure. Surveillance breeds workarounds; partnership builds judgement.

Q9: C — Sextortion against minors is a federal crime. Stop responding (engagement escalates), document, tell a trusted adult, report to FBI/IC3.

Q10: B — Quarterly cybersecurity family check-ins normalise the conversation. After news events (breaches, scams) reinforce. Builds collective resilience.

Scoring

Score	Level	What it means
0–4	Beginner	Your family's collective defences are weak. Run the Family Online Safety Plan Worksheet and the Family M
5–7	Intermediate	Solid family awareness. Use the Family Device Rules Template and Online Safety Agreement to formalise.
8–10	Advanced	Strong family security culture. Make sure to include extended family (elderly, college kids) in your defence