1. Wait for independent experts to weigh in.
2. If a story reveals security holes, ask who is most likely to be affected.
3. Beware language that ignores the likelihood of an attack.
   - Absolute language (e.g., “unbreakable encryption”)
   - “Can,” “could,” “able to,” or “it’s possible to…” (e.g., “if they want to get in, a burglar can ram a Toyota through your front door”)
4. Don’t lean on one opinion. Look for the consensus of experts within and across stories.
5. Ask how expensive the threat really is. (Time, effort, financial, legal, technical resources)
6. Beware marketing terms. (e.g., “NSA-proof,” “military grade cryptography”)
7. Know who to trust. Understand the political leanings and motivations of software creators.
8. Lend trust to open source software, especially when tested under security audits.
9. Don’t judge software developers on the existence of vulnerabilities — judge them on how they respond.