File 20090211.1240: Ka-Ping Yee's nine principles for secure systems [1, p. 289]:

- Things don't become unsafe all by themselves. (Explicit Authorization)
- I can know whether things are safe. (Visibility)
- I can make things safer. (Revocability)
- I dont choose to make things unsafe. (Path of Least Resistance)
- I know what I can and cannot do within the system. (Expected Ability)
- I can distinguish the things that matter to me. (Appropriate Boundaries)
- I can tell the system what I want. (Expressiveness)
- I know what Im telling the system to do. (Clarity)
- The system protects me from being fooled. (Identifiability, Trusted Path)

I think the most common computer systems today violate every single one of these. Ivan Fléchais doesn't like them very much. He suggests, as a game, to try negating each one and see if it makes sense.

References

[1] Ka-Ping Yee. User interaction design for secure systems. In *Proceedings of the 4th International Conference on Information and Communications Security (ICICS '02)*, pages 278–290, Singapore, December 2002.