10 Commandments of Hacking

Below are the 10 commandments of hacking, as seen in the October 22, 1990 issue of Spectrum online newsletter, Issue #1. It is included in the original font format of the time.

Note the focus on avoiding getting caught doing illegal activities, not on proper ethic as we view them. The following would be considered an unacceptable set of ethics for modern Information Security professionals.

```
                    - The Ten Commandments of Hacking -

    These are the ten rules of hacking that I go by when I hack around on
systems.  These rules are important in order maintain from being caught or
discovered illegally hacking on a system.

I.    Do not intentionally damage *any* system.
II.   Do not alter any system files other than ones needed to ensure your
      escape from detection and your future access (Trojan Horses, Altering
      Logs, and the like are all necessary to your survival for as long as
      possible.)
III.  Do not leave your (or anyone else's) real name, real handle, or real
      phone number on any system that you access illegally.  They *can* and
      will track you down from your handle!
IV.   Be careful who you share information with.  Feds are getting trickier.
      Generally, if you don't know their voice phone number, name, and
      occupation or haven't spoken with them voice on non-info trading
      conversations, be wary.
V.    Do not leave your real phone number to anyone you don't know.  This
      includes logging on boards, no matter how k-rad they seem.  If you
      don't know the sysop, leave a note telling some trustworthy people
      that will validate you.
VI.   Do not hack government computers.  Yes, there are government systems
      that are safe to hack, but they are few and far between.  And the
      government has infinitely more time and resources to track you down than
      a company who has to make a profit and justify expenses.
VII.  Don't use codes unless there is *NO* way around it (you don't have a
      local Telenet or Tymnet outdial and can't connect to anything 800...)
      You use codes long enough, you will get caught.  Period.
VIII. Don't be afraid to be paranoid.  Remember, you *are* breaking the law.
      It doesn't hurt to store everything encrypted on your hard disk, or
      keep your notes buried in the backyard or in the trunk of your car.
      You may feel a little funny, but you'll feel a lot funnier when you
      when you meet Bruno, your transvestite cellmate who axed his family to
      death.
IX.   Watch what you post on boards.  Most of the really great hackers in the
      country post *nothing* about the system they're currently working
      except in the broadest sense (I'm working on a UNIX, or a COSMOS, or
      something generic.  Not "I'm hacking into General Electric's Voice Mail
      System" or something inane and revealing like that.)
X.    Don't be afraid to ask questions.  That's what more experienced hackers
      are for.  Don't expect *everything* you ask to be answered, though.
      There are some things (LMOS, for instance) that a beginning hacker
      shouldn't mess with.  You'll either get caught, or screw it up for
      others, or both.
```