Physical Security

scenario: somewhere in this building, I have a lab with computers
    your job is to bring back a file that's on one of those machines that lists my online passwords
direct access to a machine is not always possible
but if it is, it becomes much easier to gain access
did you think your windows machine was secure?
    trinity boot cds
        unlimited access to a windows box using a USB stick
        it tech's use this because most people don't have access to the admin account
    sony rootkits
        billed as copy protection because what you purchase isn't really yours
        software put on their CDs
        automatically installed (rootkit) on windows machines when you play their CD
        it interferes with the normal way windows plays CDs
            it didn't affect other OS (now you know why I don't use windows)
        the rootkit creates vulnerabilities that other malicious software can exploit
            like gaining complete control over your system
            just because you bought a sony CD
        big time lawsuits filed over this
        CDs recalled; sony slapped on the wrist
        and you know what? The rootkit was written with code licensed under GNU GPL
        the problem was that this was secretly done without your permission
I might just grab your HDD and hook it up to my netbook
    mounting drives in linux livecd (e.g., Knoppix)
    I can quickly image it and take a look at its contents later
    and you won't even know about it
    we can even hook up your HDD to a modified USB stick and copy its contents through USB
        IDE2USB
without physical security, nothing can stop someone from getting at your system/data
    even on linux systems, we can quickly modify grub (bootloader) to bypass login password