Prevent unauthorized boots and system access

Many computers are kept in places where casual passersby may have an opportunity to access the computer, unobserved for short periods. In addition to physical precautions to prevent or slow computer theft (such as locked cases, alarms, and security cables similar to those used to slow bicycle theft), [precautions](http://www.pcworld.com/article/114727/lock_down_your_pc.html) should be taken to prevent an unauthorized operating system from being booted using an external device (such as USB drive). Once such as external OS is booted, it can be used to access most hard drive(s) on the computer and the contents copied to a second external device (to be examined or unencrypted later). This is a common means of data theft that is fast and easy to accomplish, and means to deter it should be taken on any public or semi-public computer.

* Set BIOS to restrict bootup to the hard drive only.
* Set a Supervisor/Administrator password for your computer's BIOS. (I recommend writing it down and taping it to the inside cover of the computer case prior to locking the computer case.) Disable booting from all devices except the hard drive. Setting the hard drive as the first priority boot device is not enough, as most current BIOS menus allow manual selection of any enabled boot devices. Only the hard drive should be left enabled.
* Enable Hard Drive locking, if your computer's BIOS allows it. Most hard drives allow a password to be set by the BIOS and stored in a chip on the hard drive controller which can only be reset by disassembling the hard drive. (Some manufacturers provide a backdoor security key, however.) BIOS versions found on newer computers/laptops allow this password to be set in the BIOS, so that only a BIOS containing the correct password can unlock the hard drive. (If the hard drive is then removed from the computer, it cannot be accessed by any BIOS that does not have the correct password or backdoor security key.) Note, however, that this precaution does not protect against booting from external devices if the BIOS is still set to allow that.
* There is a risk to this security measure. If you forget the password and the BIOS passwords somehow get reset, the hard drive would become inaccessible. The BIOS and Hard Drive password(s) should always be stored in a safe location.
* Password protect the Grub bootloader. Without password protection, Grub can be used to circumvent BIOS restrictions. See this section for [Grub Legacy](http://ubuntuguide.org/wiki/Ubuntu_Precise_System_Administration#Protecting_Grub_Legacy_from_cracking) and this section for[Grub2](http://ubuntuguide.org/wiki/Ubuntu_Precise_System_Administration#Protecting_Grub2_from_cracking).
* Make sure all user accounts are protected by a [password](http://ubuntuguide.org/wiki/Ubuntu_Precise_Privacy#Passwords_and_file_authentication), and always require passwords for login. Never create an "administrator" user account (hidden or not) and leave it unprotected by a password. Never enable automatic login without a password to any user account.
* It is possible to enable [automatic login](http://ubuntuguide.org/wiki/Ubuntu_Precise_Tips#Automatic_user_login) to a preferred password-protected user account while simultaneously enabling a password-protected screensaver (the password for which must still be entered even before initial user access). This is a reasonable solution that offers protection while still allowing automatic login.
* Make sure a password-protected [screensaver](http://ubuntuguide.org/wiki/Ubuntu_Precise_Utilities#Screensavers) is always enabled (that will engage after a reasonably short period of inactivity).