Keeping your computer and personal information safe from security threats is one of the most important aspects of computing today. This guide aims to help you achieve a higher level of security. Pay particular attention to the following subsections:

Keep your software up to date

Use strong and unique passwords for important accounts

Do not run scripts or install applications from unknown sources

Keep your browser clean for sensitive activities

Remember email security

Keep your software up to date

Security updates are very important. They are the best defense you have against the people who want to harm your computer, and you should install them immediately. When a security update is released, hackers already know how to abuse computers that are not up-to-date. In the worst case scenario, they are searching for victims to hack with automated programs in under a few hours.

Automatic security updates are enabled by default in Black Lab Enterprise Linux. If you want to change the settings for the automatic updates, go to the Updates tab under → Settings Manager → Software & Updates and change the settings to your liking.

[Warning]
Disabling automatic updates lowers the security level of your computer. When the automatic updates are turned off, it is essential to remember to manually upgrade often.

[Tip]
If you use an Internet connection with limited bandwidth and do not want to use automatic updates, remember to update every time you have access to an unlimited connection.

Passwords

[Warning]
Official companies will not ask you for your password. If you are asked for your password, delete any e-mail asking for such. If you are on the telephone, hang up and call someone you know to ensure that the connection to those asking is lost.

Use strong and unique passwords for important accounts

Using strong and unique passwords for important and sensitive accounts helps prevent unauthorized access to your personal information, identity theft and direct financial losses.

Password reuse can turn into a disaster. You should pay attention to use unique and strong passwords for the following services:

Email accounts. Email accounts can be used to reset all your other passwords via the “Forgotten password” links found on all websites.

Key stores and password managers. It is worth having a good password for those services, since they allow you to avoid typing many other passwords!

Accounts related to banking, including PayPal and other payment sites. If someone can access these, they can steal your money.

What is a strong password?

The strength of a password depends on how hard it is for an attacker to guess it. Attackers use special programs that can make millions of guesses per second, so weak passwords don’t stand a chance.

Some passwords (like monkey , password , test , 123456) are extremely common. If you use those common passwords, your accounts will be hacked easily. However, adding capital letters, numbers or symbols is often not enough to turn a weak password into a strong one. This is because people reliably pick the same additional symbols and numbers (for instance, monkey1 is more common than mo5nkey , and also more common than monkey hoover).

It is better to choose a longer secret, such as a pass phrase (for example correct horse stable battery), than a secret that is both hard to remember and easy to crack. Consider using a series of common words which you can easily remember. Do not pick words that people around you would naturally associate with you (for instance, you should not pick poker related words if you play poker every day).

How to reuse passwords safely?

While using the same password for multiple accounts is not encouraged, everybody ends up doing this, even security experts. However, many commonly used websites get compromised by hackers every year. Some of them might even purposefully sell their users' passwords to third-parties. There is no definitive agreement among security researchers on how to reduce the risk of reusing passwords, but you should consider the following:

Separate your professional password from your personal passwords.

Avoid mixing passwords between websites where attackers can damage your reputation and low-value websites.

Use a password you're willing to lose for sites you do not trust.

Do not "waste" passwords on websites you connect to once a year. Make up a random password and use the "forgotten password" feature next time.

When to change your password?

You don’t need to change your passwords every other day. In many cases, if an attacker can steal your password, they will be able to steal it again in the future.

If you do need to change your password, you must pick one that is actually different from the previous one. For example, monkey5 is not an acceptable substitute for monkey4 , and it will be easily guessed by an attacker who already stole your previous password!

How to change your login password

To change your password, follow the steps below:

Open → Settings Manager → Users and Groups

Click on your username on the list

Click Change... next to the Password label

First enter your Current password

Now you can either

Generate a random password by selecting Generate random password and pressing Generate

Choose your new password yourself by typing the new password to the New password and Confirmation fields

Finally, click OK to confirm the password change

[Caution]
While it is possible to make Black Lab Enterprise Linux log in automatically on boot within the user dialog, automatic login is highly discouraged because it provides less security for your system.

Please turn on automatic login on only if you can trust everybody that has access to the computer.

Watch out for stolen passwords occasionally

Websites like haveibeenpwned.com can tell you if your email address or username appears amongst databases of stolen passwords. It is a good idea to check it every other month. Besides, you may occasionally hear about a service you use in the news, or get an email from a service provider informing you that they have been hacked. When you are confident that a password has been compromised, you should:

identify all the services where you used that password

change your password on all those services

verify the recent activity on the concerned accounts (watch out for money transfers; also, email services often keep a log of your recent connections with IP addresses and locations)

[Warning]
Never reveal your password to a third-party website. The website above is OK to use because it asks for an email address, which is relatively public information. It does not ask for a password. Websites that ask for your password will most likely misuse it.

What about password managers?

Password managers are a very convenient way of using many unique passwords without having to remember them all!

[Tip]
There are several password managers available in the repositories, including KeePassX and PaSaffe.

Some password managers, like KeePassX can synchronise your passwords across devices, including Windows or OS X computers. You should be aware of a few limitations, if you decide to use a password manager:

Online password managers can be hacked too. Do not store your email or bank passwords in a password manager.

Use a memorable password to unlock your password manager! If you lose that password, you could end up losing access to all your accounts (another good reason not to store emails in your password manager).

Proprietary password managers should not be trusted. Nobody knows what they do with your passwords.

You may need to use some accounts from your friends or family’s devices. For those accounts, you can tell your password manager to use a specific and memorable password instead of a random password.

If you keep the above advice in mind, password managers can be a great way to stay more secure, more easily!

Tips for good online security

Do not run scripts or install applications from unknown sources
Install applications from the repository whenever possible.

When running a script found on a troubleshooting or support website or given to you on IRC, take a moment to look at it, or ask a third-party to confirm what the script does. Be especially wary of scripts that require root access, as they could compromise other users' accounts.

Keep your browser clean for sensitive activities

Web browser extensions are a popular mechanism among hackers for harming users. They are especially relevant to Linux, since they are compatible with all platforms. Malicious extensions could steal your passwords, monitor your activity online for advertising, abuse your social media accounts or steal your money.

You can take measures to limit the risks you expose yourself to:

Never install an extension that is not distributed by your browser vendor

On Chrome and other browsers, use the Incognito mode for sensitive activities like banking and e-shopping. Incognito mode disables extensions.

Remember email security

Do not open email attachments from people that you don’t know, or if you think the content of the email is incoherent or suspicious (for example invoices coming from people you have never heard of).

Do not reply to spam. This will inform spammers that your email address is active, and it will incite them to send you more spam.

Consider firewalls if your computer hosts Internet services
If you run public facing Internet services, or are not on a NAT, you should consider using a firewall. Most home users are not concerned by this measure.

Understand that firewalls are not very useful in their default settings. You should consider what you want to achieve and configure the firewall accordingly. Firewalls can protect you against denial of service attacks, limit access to a service to specific IP addresses or inspect and reject suspicious packets. However, they cannot protect you against unknown or emerging threats, and they do not replace the need to install security updates.

Back up on a regular basis

A problem that you may occasionally encounter is the unexpected loss of some of your work and settings for one reason or another. The causes of such data loss are many and varied; they could be anything from a power failure to accidentally deleting a file. It is highly recommended that you make regular backup copies of your important files so that, if you do encounter a problem, you will not have lost those files.

It is wise to store backup copies of files separately from your computer; that is, you should make use of some form of file storage which is not permanently attached to your computer. Options include but are not limited to writable CDs and DVDs, external hard disks, USB disks and other computers on the network.

A simple way of backing up your files is to manually copy them to a safe location (see above) by using the File Browser as well as the Archive Manager which lets you compress files and pack them together. Alternatively, you can use a dedicated backup application.

General advice on how to keep good backups:

Back up on a regular basis

Always test your backups after you make them to ensure that they have been made correctly

Label your backups clearly and keep them in a safe place

[Tip]
There are numerous dedicated backup applications available in the repositories, including Dejà Dup and luckyBackup.

[Tip]
If you use online backup services like Dropbox, it is a good idea to first encrypt your documents and upload an encrypted archive. This will prevent the online services staff from accessing your documents.

[Tip]
Backups can also be an effective protection against ransomware, which encrypts your data and will only decrypt it if you pay the developers. To keep clean from ransomware, avoid installing applications from unknown sources. For more information, see Do not run scripts or install applications from unknown sources.

Consider encryption

Full disk encryption is a good measure to protect your computers content should it get stolen. You should consider it if, for instance, your job involves valuable Intellectual Property or executive responsibilities. Remember that full disk encryption will not protect you if you do not shutdown your computer when you are not using it.

[Tip]
The easiest way to enable full disk encryption is to do it during the installation.

Using your computer in a shared environment

Do not use shared accounts

When Black Lab Enterprise Linux is installed, it is set up for a single person to use. If more than one person will use the computer, it is best for each person to have their own user account. To read more about adding users, refer to Users and groups.

Lock your screen while away

Locking your screen prevents other people from accessing your computer while you are away from it. All of your applications and work remain open while the screen is locked.

To lock the screen, press Ctrl+Alt+Delete or click → Lock Screen.

To unlock the screen, move the mouse or press a key. Then, type your password and either press the Enter key or click the Unlock button.

If more than one person has a user account on your computer and the screen is locked, other users can press the triangle button to the right of the user name, select their name from the list and enter their password to use the computer, even while the screen is locked. They will be unable to access your currently open work and you will be able to switch back to your locked session when they have finished using the computer.