HandyLinux, based on debian, is a particularly **stable and secure system**.
In graphical typical mode use, you do not risk anything.

HandyLinux & Security

The GNU/Linux systems have reputation to be **insensitive to virus**...
but the danger still exist... A **virus**, a **malicious command** can perfectly fit in an attachment, link or software downloaded from the Internet.
With a few simple habits you can easily **protect your system and data**.

This page is not a complete wiki about security, simply a series of tips that will save you 99% of security incidents.

Protect your system

physical Security

This is obvious, but to say once: If you want your data protected, **do not leave your laptop computer anywhere ! Do not let your computer in self-service at home !**
Your computer contains passwords to banking sites, traces of most of the sites you have visited, etc...
If you want to make discover your distribution or simply share its resources, I suggest you to create an additional user who will not have access to your data or to administration system.

Updates

Updates your programs provide features, correct bugs, but more importantly **correct possible security vulnerabilities**.
This is the great strength of the free-software community: program sources are available, so when a vulnerability is discovered, it is made public and corrected in the wake...
Unlike proprietary systems flaws which kept secret, continue to poison the users's life...
With HandyLinux updates are automatically detected and an orange/red icon appears in your task-bar notification area prompting you to update your applications.
All details in the relevant section.

Password

Each year tens of thousands of email accounts, WiFi access, PIN codes... are easily hacked because users have chosen a password too easy to guess.
Palm of the worst 2013 password go to **123456** , but without relying on other smokers as a result **AZERTYUIOP 0000**, animal names, birth dates...
All these words are too simple to be avoided!
It is also not by adding two simple password that you create a good one ! A “crumble50” will certainly hardly discovered by a human, but a “computer robot” decipher this code very quickly, trying all words in different dictionaries and all suites figure.

To increase the robustness of a password, that is to say, its resistance to attempts to decrypt, use the most possible characters and vary their type (lower-case, upper-case, numbers, special characters)

Mnemonic method

Here is a simple, but very effective method to create a good password, but also get to remember easily :

1. Find a sentence, a quote, a chorus; for example: “three little pigs are walking in the forest”.
2. Take the first letter of each word : **tlpawitf**
3. Add it numbers, upper-case and special characters.
   Caution ! Stay logical with the positioning of these, otherwise you will not remember your password !

A simple mnemonic solution (but you invent other) is to replace certain letters with some numbers or special characters, for example:

letter	associated symbol
l	£
e	€
s	$
o	0
i	!
a	@
and	&
two	2

“three little pigs are walking in the forest” give, following this method : **3£p@w!tf**
You just create a good password !

Using this method, the more paranoid of you may increase the number of characters in their password, simply by finding a longer sentence, or why not a poem if you have memory.

Caution, even if your password is good, it should never be used on several sites!
You can use different sentenses related to the site, using the same method :

- You want to connect to Facebook. For example remember: “I know full of people on Facebook,”

which gives "**!kfOp0f**"
- You want to connect to Gmail. Remember: "Gmail spying all conversations and resells informations", which gives "**Gms@c&r!**"

Otherwise take back to your previous password "three little pigs are walking in the forest", and add a small sentence in connection with the site on which you want to be identified. For example:

website	password
Facebook	3£p@w!tfF@C€B00K
Gmail	3£p@w!tfGM@!£
HandyLinux	3£p@w!tfH@NDYL!NUX

Finally, if you really want to ensure the strength of your passwords, do not save them in the browser, type each time.

Scientific method

A different approach for those who have no mnemonic memory.

1. **Install a password manager** like keePassX. This software protects your passwords with… a password of course !
   To install on HandyLinux, use the Debian software center, type "keepassx" in the search area, then "install".
2. **Generate your passwords** : Go to this website and bottom, click on "generate"
3. **Centralize your passwords** in a manager stating clearly what they correspond !
4. **You can use Passwords and keys** (seahorse) to create and manage PGP keys and passwords and key SSH.Mots provides an interface to most of the functionality of Gnu Privacy Guard (GPG) and integrates with several desktop components . to install it, open the Software Center (HandyMenu / Raiders / Debian Software Center and search for "Passwords" you will have more passwords and key choice for other management software Passwords.

Protect your datas

Restrict access to your data

If you use HandyLinux in "multi-user", you may want to restrict access to your data to other users. The procedure is very simple and is done graphically (no need to open the terminal). All information on the dedicated page in the documentation.

Backup your data

If you have visited this documentation, you have certainly see this kind of bubbles :

Back up your data before ….

And it is not for nothing. Whatever your level on computer or your equipment's condition, no one is safe from misuse, technical incident, violent storm, cup of tea on the keyboard , a cat that relieves itself in the central unit...

To preserve your important data, several solution exist.

Warning! The “cloud” is all the rage right now ... Several online services are available to you to paste your personal data to an external server for which you have no control ... What's for an idea to “protect “your data!
First, you are not immune to an incident on the server,
secondly, you have no real control over the top use of your data.

I strongly advise you, when in doubt (all services “cloud” are not subsidiaries, which the NSA ...), back up your data “locally”, on physical media owned by you and for witch you have total control.
To preserve your data, the HandyLinux documentation offers a full page about synchronisation and backup of your data.

Anti-Virus software

Certainly, the GNU/Linux systems are much less susceptible to viruses, but a virus on GNU/Linux stay possible if you don't use regular repositories.
ClamAv is the reference anti-virus software for GNU/Linux. A complete documentation already exist on the wiki Easy-Debian. I let you consult the excellent article about Clamav on Easy-Debian.

Parental Control

Yes, you can find everything on the internet, the best and the worst, and often inappropriate images or content to our children. To let your children enjoy the digital world safely, you can use different parental control systems.
But keep in mind that the best parental control is you !

From your Internet Service Provider

Your Internet service provider offers various parental control software. Those systems enables control over all positions of the house, but does not exempt activate parental controls on your internet browser.
Consult your specific ISP documentation for more information.

From your computer

The establishment of a parental control is for advanced users because the procedure is complex ... and not 100% effective.
In addition the “forbidden sites” should be updated regularly.

HandyLinux is a distribution for beginners, I'll let you visit the Debian-fr forum dedicated thread.