The Internet is certainly an extraordinary tool for communication, information, learning and development. This virtual space nevertheless conceals risks, the majority of which are the result of negligence in the use of personal data.
It is therefore important to adopt a vigilant attitude when using the Internet and to think twice.
before sharing or publishing information on the net or installing software on equipment
computer science.
Without being exhaustive, these tips will help you take advantage of the multiple advantages of technologies.
of Information without exposing yourself too much to the threats that threaten your assets
informational.

Adopt good practices

- Protect your information system against new threats by updating periodically virus signature files.
- Do not forget to regularly apply software updates (operating system, browser, database manager, etc.). They make it possible to correct the flaws security and prevent exploitation of corresponding vulnerabilities.
- Secure access to your wireless network by choosing a password and a protocol strong encryption.
- Change the default passwords corresponding to the administrator accounts of the hardware and computer software used (router, PC, RDBMS, etc.).
- Set up a security policy allowing the management of access rights to your information heritage.
- Regularly analyze your event logs.
- Include a confidentiality clause in contracts signed with partners (employees, suppliers, subcontractors, etc.).
- Deactivate the access codes of former employees.

Warning ! logins and passwords are entry points to your heritage informational

- Choose complex passwords. Preferably a combination of at at least eight characters including upper and lower case letters, numbers and special signs;
- Change passwords periodically;
- Do not allow browsers or mobile apps to remember important information such as password, card number, credit, etc.
- Make sure that unused sessions are closed or locked.
- Prohibit passwords from being written on paper, accessible to unauthorized third parties.

And for cloud computing

- Establish, with the service provider, a contract guaranteeing the security of your information heritage.
- Choose a service provider that uses servers installed in countries that provide sufficient protection of personal data.
- Avoid storing confidential data in the cloud. If this is not possible, think to encrypt them.
- Require a clause and a portability procedure allowing you to change the provider or, where applicable, repatriate your data to your own servers.

Educate your employees about privacy protection

Think carefully before sharing

The Internet has no borders. Paradoxically, he has a very good memory. It is therefore imperative assess both the interest and the risks associated with sharing content that may expose his or her private life, those family or the information assets of their employer.

Comments, ratings, reviews, photos and videos

- Post in moderation any type of content that may reveal your racial or ethnic origin, your political opinions, your convictions religious or philosophical, your union membership, your state of health, your movements, etc.
- Limit access to the content you publish to your knowledge.
- Avoid posting photos or videos that identify other people without their consent.

Please note, simple clicks can lead to legal action

- The apology for crimes.
- Diffamation.
- Illicit access to information systems, etc.

facebook.com/CNDP.Maroc/ twitter.com/CNDP_Maroc

Address: Angle Boulevard Annakhil and Avenue Mehdi ben Barka, Immeuble Les
Patios, 3 rd floor Hay Riad - Rabat Morocco - Tel: 05 37 57 November 24 - Fax 05 37 57 21 41
Website: http://www.cndp.ma