Aller sur **mtn.cm (https://www.mtn.cm)** | **MTN Community (https://community.mtn.cm) (/en/support/home)**

Best practices on internet

Modified on: Mon, 11 Mar, 2019 at 10:56 AM

Computer users are increasingly numerous and these computers are usually connected to networks, particularly the Internet. If these users do not take minimum precautions, their computers can easily get attacked. As such, Ten Commandments are here to guide you. They are:

1. **Use quality passwords**. The dictionary defines a password 'as an agreed formula destined to be recognized as a friend to open a guarded passage". A computer password provides access to the computer and the data it contains. It is therefore important to choose quality passwords that will be difficult to get access by using tools and very difficult to be guessed by a third party.

2. **Have an operating system and updated software: browser, antivirus, desktop, personal firewall, etc.**
   Most attempted attacks arise as a result of faults inherent in a computer (operating system or software faults). Generally, attackers look for computers whose software has not been updated to use the fault to launch an attack. This explains why it is essential to update all the software so as to correct these faults.

3. **Do regular updates.**
   One of the first principles of defense is to keep a copy of your data in order to respond to an attack or a malfunction. Backing up your data is a condition for the smooth running of your business.

4. **Deactivate ActiveX and JavaScript components**
   ActiveX or JavaScript components permit the proper functioning of certain features but can also bring about security risks that can be perpetrated by an intruder to a vulnerable machine. Despite the inconvenience this may cause, users should deactivate their information that were sent unconsciously and make sure it is activated only when you are sure you are using a trusted website.

5. **Don’t be in a haste to click on links**.
   Attacks aim at deceiving Internet user to steal personal information arises as a result of clicking on the link that appears on the message. This link may be misleading and malicious. Rather than click on it, it is better to enter the website address in the browser address bar. These shall prevent so many problems.

6. **Never use an administrative account to navigate**.
   A computer user has privileges or rights. These rights do permit and at the same time do not permit control of certain actions and access to some computer files. These rights are generally called Administrator rights and at times called simple user rights. In most cases, every user has the right to send enough messages and to surf the internet. By limiting the rights of a user, we also limit the risk of infection or compromise of the computer.

7. **Control the dissemination of personal information**
   The internet is not a place where you can be so confident since the information you leave can escape instantly! In this context, avoid leaving personal data without closing them. Don’t forget to log out to your personal and sensitive information (such as bank details) that are found on the Internet. In case of doubt, better stay away from it.

8. **Never leave jokes.**

Never leave jokes as messages or some sort of string letters, instead lay emphasis on financial transactions, solidarity calls, virus alerts, etc. Whoever the sender may be, rebroadcasting these messages may bring about confusion and saturate the network.

9. **Be careful:**

The internet is a locality that is populated by strangers! We must remain vigilant! For instance, if a well-known correspondent and the person with whom we exchange regular mails in French sends a message with a title in English (or any other language, don't open it. If you doubt this message, always try to confirm the message by calling. Generally, do not entirely trust the sender that appears in the message and never reply messages from strange people.

10. **Be careful while opening attachments to an e-mail: they often have malicious codes**

One of the most effective methods to disseminate malicious codes is to use files attached to e-mails. To protect yourself, never open attachments with the extensions: .pif (for example an attachment called "photos.pif); .com, .bat, .exe; .vbs, .lnk. On the other hand, when you send files as attachments to e-mails, make it a habit to send attachments on "inert" format, such as RTF or PDF for example, this shall limit the risk of information leakages. Source : **ANTIC (https://www.antic.cm/)**

P Paul is the author of this solution article.