alpha numérique

SUMMARY

Online security : Tips and tricks

Introduction

Online security is all over the digital experience. Discover ready to use tips and tricks to protect yourself better and to develop good reflexes as users. In this summary, we will see which data we need to protect and we will discover the basic tools to guarantee our online security.

In this document, the padlock symbol is used to measure approximately, the level of protection associated with each solution that we suggest. The fewer padlocks there are, the easier it would be to hack the data that needs to be protected if you refrain from using this protection solution.

What is the personal data that I need to protect?

DATA THAT NEEDS TO BE PROTECTED MIGHT BE SAVED ON MY DEVICE.

- Scanned administrative documents.
- Private data or photos.
- Sensitive professional data.

I HAVE THE RIGHT TO LEAVE SOME TRACES WHEN I "BROWSE" ONLINE.

- My identity.
- The purchases that I make.
- The websites that I visit.

I USE THE INTERNET TO COMMUNICATE PERSONAL DATA CONSCIOUSLY.

- Emails
- Follow-up of my bank accounts and governmental agencies
- Communications on social networks

How to protect my device?

I make sure that my device remains in my possession and that a malevolent person does not have access to it.

- Beware of leaving any devices unattended.
- Beware of carrying devices everywhere.
- Consider localization and remote locking solutions.

I must use passwords or passphrases to lock my device and my software.

- As for your device, consider the settings associated to passwords, such as auto-lock.
- As for your software, consider password managers such as *Keepass* (free), *LastPass* (free)…
- Although restrictive, double authentication reinforces security.

I can use an antivirus (ex.: *Avira, BitDefender, Avast*).

- Protection from malicious software *(malware).*
- Protection from unwanted software that infiltrates your devices *(spyware).*
- Protection from input and output to the computer: Firewalls.

I can encrypt sensitive files that I keep in my device.

- Encryption is similar to a digital safe.
- There are a lot of encryption software that you can get for free (ex.: *AxCrypt, VeraCrypt*)

How can I protect myself when I browse the web?

I have to browse the Internet by using secure connections: HTTPS!

- HTTP is a data transfer protocol.
- HTTP**S** is the secure version of HTTP.

I can refuse the use of *cookies*.

- Cookies allow us to personalize our Internet experience and offer great comfort when browsing.
- Cookies disclose our personal data and our habits to private companies.
- The analysis of this behavioural data is sold and bought by private companies.

If I want to remain anonymous, I can avoid connecting myself frequently by using login credentials.

I can use remote access servers or *proxies* to simulate the fact that I connect myself from a different location and thus, making my IP address difficult to trace.

- The Virtual Private Network or VPN allows to simulate a connection from a different location.
- Browsers that anonymize, like Tor, use many proxies automatically before connecting you to the website that you want to access.

How can I protect the data that I want to communicate on the Web?

I make sure to control or be aware of my audience.

- Who can see the information that I upload?
- How much can I trust that audience?

On Facebook, for example:

- https ://www.facebook.com/settings?tab=privacy
- https ://www.facebook.com/settings?tab=timeline
- https ://www.facebook.com/settings?tab=followers

I try to make sure that the content that I communicate does not harm me or does not harm others.

- Is it really necessary to publish my date of birth, my telephone number, my address, my workplace, etc., online?
- Who owns the information that I publish on the social networking site?
- Which information that concerns me can any of my contacts transfer to other parties?

On social networks, I can use different accounts/pseudonyms according to the audience to whom I address myself (family, work, leisure).

Keep learning on alphanumerique.ca!