Knowledge Box 10

Personal Brand and Digital Identity: Keys to Privacy and Online Security

By Selva Orejón, professor of Privacy and Online Security at

INESDI Digital Business School

Identity is the set of features or characteristics of a person that may be separated from others in a set. Therefore, digital identity is the set of information, features and characteristics that we share online as well as the trail we leave on different social networking sites, professional profiles, blogs, company pages, comments we make in news, reviews, forums, etc. By putting together these tiny pieces we get a completed puzzle made up of who we are and what we do.

If we can create a set of characteristics that we leave behind online and which we actively communicate, then we must also account for the set of information shared by third parties about ourselves, whether or not we realize it, which can be considered passive communication.

This passive information and in best case scenarios we know about, can end up playing a trick on us, especially if we don't know that it's been shared and even less if we don't know where it originated from or who published it. (Tip: configure Google Alerts with your name, pseudonyms, ID numbers, current and past telephone numbers, emails, home address).

The first step to being protected and for controlling our privacy is to know what has been published about us, both active and passive information, so that we can start our Digital Identity Protection Protocol. Not all the information published about us is necessarily negative, inappropriate or of intimate nature, but we should know exactly what is shared online about us.

How is digital identity and reputation related?

We are facing an important paradigm shift in communication systems, the way we interact has changed our perception of privacy and areas of our lives that once seemed inaccessible have become, in many cases, public.

It's funny how even knowing that privacy and intimacy are things that the use of internet technologies can't guarantee we continue resisting to believe that it's okay to upload images or use the same password on all our devices and social media accounts.

We don't fully understand the danger of leaving our digital identity in the hands of others and when we finally realize that we no longer have control of our data we're helpless.

Online not everything goes, not everything can be and not everything is equal. We can, and sometimes should, remove harmful content shared online about a person, brand or surroundings. Prevention is the best defense when it comes to our security and online privacy. We must learn to properly manage both our personal and professional privacy and digital security. It's essential to master new techniques of open source searches, to know how to act in a reputation crisis, and to act quickly, safely and efficiently…

Steps for Digital Identity and Protection Protocol (DIPP)

1. Initial Concepts: so both individuals and employees of a company understand the usefullness of DIPP they must first be introduced to the basic concepts. para que tanto un particular como los empleados de una empresa conozcan la utilidad del PPID se les debe introducir a los conceptos básicos

a. Identity:

i. What is identity?

ii. What is digital identity?

b. Perso-Professional Reputation

i. What is reputation?

ii. What is online reputation?

c. Know what rights we have online

2. “What is the current professional and digital identity”

i. Identity and Reputation Agents

b. Public reputation, not media reputation

c. Know the current Digital Identity

i. Identity tools and alerts about “what is said about a persono r company online”

ii. Evaluate the digital risks

3. Protocol for detection and evaluation of a Digital Crisis:

i. Protocol for Reputational Digital Crisis

ii. Protocol for digital “issues”

iii. PNA Strategy

1. Prevent / Notify / Aid

4. Simulation Exercises

a. Domestic / Business / Public

5. Self-protection Manual: What to do about online vulnerabilities?

a. Choose our level of invisibility and maintain it.

b. Risks associated with careless management of our digital material.

c. Privacy and Anonymization: How to avoid being identified online

d. Use only one email

e. Spokesperson (pseudonym) / Using a false name as identification

f. Content shared online (information about you and those around you)

g. How do you know what appears about you online?

i. Search for keywords and information related to you in person and online

h. Create alerts about publications: Be aware of the information shared about you online.

i. Publish information about yourself online.

Simulation exercises about Digital Recklessness are recommended throughout DIPP such as: information leaks, inappropriate publications, social profile blocks, etc.

For two years, onBRANDING and Oracle initiated the implementation of the first job known as Corporate and Personal Brand Protect and Defense, a new professional profile that answers to the increasingly popular professional functions. This position should not be seen as a single person but instead a department or cabinet that can be made to work for specific needs or continuously.

We must always be alert about security and privacy as there are a number of newly detected problems arising from the mismanagement of communication, security and legalities online.

This profile or recycling of this professional profile must be defended internally and socially positioning itself not as a new trend but as a response to the needs of a new RSL-P paradigm. To do that, here is some data to help you understand its necessity:

- 40% of surveyed companies receive about 10,000 cyber attacks per day
- 69% of the 250 executives surveyed fear that this will increase and become more sophisticated.
- Cyber attacks on personal and corporate privacy top the list of organizational concerns (90%).
- Theft- damage to secrets of intellectual / industrial property (55%).
- Online fraud (85%).
- Theft and Identity Theft (35% of those studied affected)
- The cost of these cybercrimes amounts to $1 billion, and could

triple by 2020 if companies do not strengthen their defense.

After monitoring recent years we can agree with what Chema Alonso has said: “The bad guys know a lot, and if they don’t know it… they probably have money to hire those who do.”

Security and privacy must be dealt with on two levels: preventative (take the necessary precautions to avoid possible problems related to security and privacy); reactive (when there is already a problem you must know how to address it in the most effective and urgent manner).

Failure Aversion
Change in Europe

FACE

ENTREPRENEURSHIP