

Digital attitude: five key elements for participation in the digital society

*Teresa Romeu, Montse Guitert, Marc Romero and
Carles Bruguera*

Participation in the digital society

Today we are all part of and participate in a digital society in constant evolution. Now, although we consider that we master the digital technological tools, we have to take into account two main questions: how we participate in this digital society and if we do it correctly. The fact of being everywhere gives us a lot of freedom and power, but also forces us to be much more responsible.

1. The *netiquette*

The digital environment offers new ways of communicating, of participating, with characteristics different from those of other contexts. For this communication to be effective and adequate, we have to follow some rules of courtesy, which we include in the concept of **netiquette**, a code of conduct that has a double objective: to enable communicating in an educated manner and adapting the message to the communicative environment. The netiquette is, in broad strokes, the adaptation of the norms of courtesy of the real world to the digital world.

Some examples of rules or good digital behaviours would be::

- Interact and participate in debates and current issues in a respectful way.
- Do not massively forward personal emails.
- Do not abuse capital letters and incorrect language.
- Behave civically with the other users of the chats, forums or social networks.
- Do not include disqualifications and personal insults.
- Do not include images or expressions of bad taste.

2. The digital identity

Our personal attitude begins with who we are in the network: if we are who we are in life or we are another person. **The digital identity is the printing that we leave on the net with our actions or the actions related to us.** These actions, or lack of actions, end up consolidating some defining facts that end up identifying us. Our digital identity is therefore alive and creates multiple identities (personal, cultural, work, social ...) in multiple communities).

Usually when they look for us on the internet, the **image** they take of us is what they see, so the image we project on the web is key; and it is largely in our hands. However, although we can model our digital identity, **the digital world has a part of lack of control** which we must also be aware of, so it is important that we devote time to configure our digital profile.

Important !

Pretending to control 100% the modelling of our digital identity is practically impossible. What we can do is put tools and efforts to try that what we want to project is as close as possible to our intention.



Let's think!

We must be aware of:

- *What do we want to say?*
- *How do we want to say it?*
- *What communication objective do we have?*
- *Where do we want to be present?*
- *Do we want to expose any aspect of our life or a specific aspect?*
- *Are we aware of the image we project?*

3. The digital reputation

While the construction of digital identity depends on us, **digital reputation** does not depend exclusively on us: reputation depends on what others say, comment or share about us. It is moulded from the conversations and opinions of others.

The digital reputation can be positive or negative. Depends on the **actions** and **omissions** that we do on Facebook, Twitter, LinkedIn (through images, sound and videos) an idea of ourselves will be generated as a person, also affecting the professional field and the perception of values. The network can benefit or harm us.

4. Network security

The risks in the network with regard to the digital attitude are multiple: viruses, deceptive advertising, junk messages, offensive, junk mail, false alerts and all kinds of scams. It is necessary to be alert, and above all take measures of self-protection such as::

- Avoid opening emails from unknown senders.
- Make use of strong passwords and change them often.
- Avoid accessing unsafe pages.
- Be very careful when entering personal data.
- Update the antivirus.
- Have different email accounts.
- Do not connect the devices to third party equipment.
- Have a card with little money to buy online.

We must not be afraid, but we must be prepared and protect ourselves.

Almost 3 billion people use the network every day and this generates a large amount of data: **the network is the largest repository that has been created**. Who navigates, what you click, how the page moves and mouse; everything is saved in what we call **big data**.

In the end, everything depends on privacy, a value, on the other hand, transcendental in life. A fundamental right that in the network is more vulnerable; when we publish in the network we lose control over the content, and even if we delete that content is recorded and anyone can make it serve. We have to assess what we want to publish and learn to master the privacy settings of our profile.

5. Legislation in the network

The network is part of real life and therefore we have **rights** and **duties** that must be respected and fulfilled in order to live and coexist in a digital environment.

Users are covered in terms of privacy and consumption, because we have European regulations, but we are less covered in terms of computer crime, among other things because the law only acts reactive and not preventive. **Prevention, therefore, depends on ourselves**.

We must bear in mind that although the new European Union regulation obliges companies to request the consent of users before using the data and informing them in case of hacking, there is no guarantee of protection if we host the data in countries of outside the European Union.



Important !

Increasingly, companies look at the social profiles of potential candidates because they often speak more of us than a curriculum-edited curriculum can speak.



Important !

***Phishing** consists of deceiving someone through an email, posing as a bank or an institution habitually demanding, illegitimately, money or personal information.*



Let's think!

*Our footprint in the network can be recovered and the processed data, **big data**, provide valuable information to administrations and companies. Its good or bad use only depends on the ethics of those who use them.*

Attitude based on values

A citizen who is aware of the attitude and uses he makes of his data and respects the rights of other users of the network is considered a **good digital citizen**. It is also one that, thanks to the power of technology, changes and positively improves the areas of his life.

The digital attitude is key to be a good digital citizen and imply an attitude based on **fundamental values**, such as::

- **Honesty:** Never lie, be transparent. It is better not to give a data than to give a false one.
- **Confidence:** If we win the trust of the users, the relationships we establish will be more effective.
- **Solidarity:** If we understand the digital environment as a social environment, we not only have to wait to receive, but also give something in return.
- **Appreciation:** Thanking you for a comment or sharing content helps you become part of a community.
- **Respect:** You can criticize, but with respect and tolerance.
- **Humility:** Contributions enrich our opinion.
- **Flexibility:** Everything goes fast, you need to keep your mind open to changes.
- **Respectful:** with oneself and with others. Do not appropriate articles that are not yours, in this case always quote the original sources.
- **Common sense:** Do not do what you would not do outside. There is nothing better than being guided by common sense.

How we behave in the network represents a way of thinking, of walking through the digital environment as we do in life, with the aim of growing to be more effective and happier.



 *Let's think!*

Attitudes represent ways of thinking and motivations to act and, therefore, ways of acting in digital environments; the new digital culture needs new attitudes that are coherent with the digital world in order to create good digital citizens. Civic actions in the network improve social coexistence.

