THE BASQUE YOUTH OBSERVATORY

Interview with Ane Martínez Recio, instructor of the workshop "Cybersecurity or the Challenge of Taking Responsibility for our Actions".

Last year you delivered a small online workshop on "Cybersecurity or the Challenge of Taking Responsibility for our Actions". This year you are planning the same course, why do you want to repeat it?

Yes, I delivered the workshop last year when we were a couple of months into the pandemic and teleworking was taking hold. People were becoming increasingly concerned about security issues; about protecting their devices, networks, data, etc.

They were looking for the best tools to shield their systems, the best programmes to avoid being infected, or to free their systems from viruses if they had been infected.

However, few people stopped to reflect on the level of responsibility that they had as the users of these devices, of these networks, and as the creators or custodians of this data.

We must bear in mind that the digital transformation of our lives and work is here to stay. We cannot and should not believe that cybersecurity is alien to us, something that we have to delegate to third parties only. We can outsource and/or delegate certain issues, we can secure or shield our devices and networks with the help of third parties, but the goal of the workshop is to show that the key element of cybersecurity lies in the human factor.

Therefore, I believe the subject to be highly topical because the people in charge of training and educating young people have an important role to play in building and passing on #CyberEthics in an increasingly #Cybernetic society.

So, will we be talking about #CyberEthics in a Cybersecurity course?

We shall not focus the course on ethics. However, the human element will be a core aspect throughout the course. The success rate of most security breaches, no matter the cyber attack or cyber criminal involved, will be lower if the people using the targeted devices are well trained in using safe digital habits to become the best firewalls themselves.

Obviously, technical factors and the correct and optimal configuration of the devices cannot and should not be overlooked. However, the reality is that the human factor is currently the origin of 95% of cyber attacks, either by error or through ignorance.

Have the number of cyber attacks increased during this pandemic year?

Cyber attacks in Spain have increased "qualitatively and quantitatively" during the pandemic and have become more serious, according to a report by the National Intelligence Centre (CNI). Serious and critical attacks even doubled the figures for 2019.

The pandemic has imposed new scenarios on us, such as virtual meetings, teleworking, online classes, increased e-commerce, greater dependence on virtual socialising, etc. As a result, cyber threats are constantly changing, adapting to user behaviour and online trends to take advantage of them. This is why it is becoming increasingly important and meaningful to be aware of the key role of our actions in preventing and shielding the security of our devices and networks.

Accepting this responsibility requires knowledge of the risks and of the possible attitudes and resources available to deal with them; training and information and, above all, an ethical and coherent attitude between our analogue life and our digital life.

Why would you encourage people to join the workshop you will be giving in May?

Because many of the 'new habits' regarding digital uses and consumption that have become commonplace during the pandemic are here to stay and, once the pandemic is over, some of the latent dangers might become more acute, such as online scams, harassment, phishing, identity theft, fake news, etc...

The purpose of this course is to provide a framework where we can teach and learn, but above all, where we can reflect on the construction of this ethical framework, on what we can and should do and what we should not do, what actions or inactions can have security consequences.