

# CYBERCRIME: HOW TO PROTECT YOURSELF

Posted on 14/07/2022



Category: [Background](#)

Tags: [Cybercrime](#), [slider](#)



by **irina wakstein**

We live in an age of increasing access to and dissemination of information. Different technological tools allow us to know and distribute data that previously would have been unattainable. Technology is always presented as a double-edged sword, where on the one hand it opens doors to new knowledge and information, and on the other hand, it enables fraud and digital scams.

"In the past, cyber-attacks only affected large corporations. Today, we are all victims and they have become popular. They are increasingly frequent in small companies or even private professionals, even demanding small sums of money as ransom", said the international president of the World Compliance Association, **Diego Cabezuela Sancho** (pictured) during the first National Congress on Digital Fraud Prevention and Cybersecurity organised by the association on 9 June 2022 in Madrid and which saw the participation of Iberian Lawyer as media partner.

The truth is that the pandemic exponentially increased teleworking as well as the different administrative procedures, online training or e-commerce, without the population, law firms, companies and institutions being prepared to face the new risks that this entails.

## PREVENTION

Faced with this scenario, it is essential to raise awareness of the importance of implementing preventive models for cyber-attacks, as well as knowing the practical measures to protect information security. This is an essential aspect for both organisations and law firms and is closely linked to the function of compliance.

"At Madrid City Council we had planned training on digital security and, once we were faced with the pandemic reality and teleworking, we managed to transfer it to a virtual level so that all of us who work there could protect ourselves from the threats to which we are exposed day after day. It is essential that everyone within their own organisation, company or public entity is aware of the prevention and protection of their information," says **María Ángeles Prieto Arroyo**, General Director of Economy of the Madrid City Council.

Cybercrime and cyberthreats are commonplace in today's world, and fishing is one of the techniques most commonly used by online criminals to steal confidential information from individuals and companies. Fishing is mainly a social engineering attack where the offender, known as a "fisher", impersonates a company or person, usually a service provider (such as banking, telephony, electricity, water, among others) in order to obtain the victim's personal data.

**[CLICK HERE TO DOWNLOAD THE MAGAZINE AND CONTINUE READING THE ARTICLE](#)**