

COMMISSIONER REDING'S WEEKLY VIDEOMESSAGE
THEME:
"Europe must be prepared for cyber attacks"

Check Against Delivery
Seul le texte prononcé fait foi
Es gilt das gesprochene Wort

Hello again and thanks for your responses to last video and for your ideas on this week's theme.

Last time, I was addressing the issue of how to ensure that you retain better control of your personal data when surfing the web, making phone calls, or using new tools such as radio chips. Today, I want to speak about a related issue: internet security.

Many of you may have dreamt of being such a proficient computer user that you could crack the security system of your school or university and know in advance the questions of your next exam, or break into your bank's computer network and add some zeros to your banking and savings account. But the reality of **cyber attacks is nowadays quite far from being a game or a proof of intelligence and curiosity**. Cyber attacks have become a tool in the hands of organised crime, a means of blackmailing companies and organisations, of exploiting the weakness of people, but also an instrument of foreign and military policy, and globally a challenge to democracy and economy. **Imagine that a one month-long internet interruption in Europe or the US would mean economic losses of at least 150 billion euro**. Or think of your personal experience: how many of you have had to replace your informatics infected by viruses or spyware? How much do you have to spend every year on protecting your computer?

Attacks in their different appearances – spam, phishing, bottleneck, denial of service, etc. – but also potential attacks against network infrastructures may have widespread and devastating consequences on our daily life: no more electricity or water at home, rail and plane accidents, hospitals out of service, and much more. Cyber attackers don't need to spend much to be able to put our business and sometimes our life at risk: on the cyber attack market, criminals can rent a platform for spamming for less than 50 eurocents per worm or zombie per week!

This is not just theory or paranoia. In 2007, key information systems of a country of the European Union, Estonia, were attacked by thousands of computers from abroad: the websites of administrations, parliament, banks, newspapers and broadcasters were swamped. This has happened in a similar way in other countries and regions of the world.

This week, I am in Estonia with ministers and experts to work on a better coordinated cyber security strategy for Europe. **So far, the EU's 27 Member States have been quite negligent. Although the EU has created an agency for network and information security, called ENISA, this instrument remains mainly limited to being a platform to exchange information and is not, in the short term, going to become the European headquarters of defense against cyber attacks.**

I am not happy with that. **I believe Europe must do more for the security of its communication networks. Europe needs a "Mister Cyber Security" as we have a "Mister Foreign Affairs", a security tsar with authority to act immediately if a cyber attack is underway, a Cyber Cop in charge of the coordination of our forces and of developing tactical plans to improve our level of resilience. I will keep fighting for this function to be established as soon as possible.**

But you also have an important role to play to improve our capacity to resist cyber attacks. Your computer may be used to attack someone else, to infect other computers, your neighbour's or a computer at the other end of the world. Internet is an open network: this means that you are also a key player in the daily fight for cyber security. You have your part of responsibility!

Ensuring resilience and security of the internet is a key public policy objective. Together with other issues, it is at the centre of the ongoing discussion on what is known as **the governance of the internet**. I will speak about this next week.

As always, your comments are welcome. Thank you for watching and hope to see you next week!