October is ECSM month!

What is ECSM?

Month of October is a dedicated ECSM (European Cyber Security Month) campaign in EU / EEA member states to get people to realize the dangers of attacks on networks and information focusing on education, information sharing and how best to protect against risk. The campaign is managed by ENISA. [https://cybersecuritymonth.eu](https://cybersecuritymonth.eu)

What is ENISA?

ENISA (European Network and Information Security Agency) is an agency of the EU headquartered on the island of Crete in Greece. Its role is to prevent and tackle the problem of network and information security in cooperation with member states. ENISA also assists the Commission with the updating and development of EU legislation in the field of network and information security. [https://www.enisa.europa.eu](https://www.enisa.europa.eu)

What is CECUA?

CECUA is an independent association that offers expertise regarding the views and concerns of users of information technology, both personal and enterprise users, expertise that takes into account the interests of users vis a vis fellow citizens, Governments, industry and the diversity of countries and regions in Europe. CECUA is registered in Belgium with an office in Iceland. CECUA is an ECSM partner in Europe. [www.cecua.eu](http://www.cecua.eu)

CECUA and its partners recognized from the conclusions of the 1998 Brussels conference “Citizens in the Global Information Society” organized by CECUA and supported by the EU that Europeans were failing to take advantage of the considerable benefits that are available from the Global Information Society because of doubts and fears arising from the Information Age.

To address these fears, CECUA and its Partners proposed a draft set of basic rights for Citizens of the Information Society in order to make policy makers and politicians aware of the issues so that they could address these fears and concerns, the Bill of Rights for the citizens of the Information society [userbillofrights@cecua.eu](mailto:userbillofrights@cecua.eu)

awareness to security. CECUA is a member of EIF (European Internet Forum) and contributed to the EIF Digital World 2030 report focusing on user issues [https://www.eifonline.org/digitalworld2030](https://www.eifonline.org/digitalworld2030).

Users and their use of technology is the key to innovation and growth. Also to the success of the digital internal market. It is not enough to leave everything to the “industry who knows best”, an old EU terminology. This is 20th century thinking; we need a 21st century thinking one.

**ECSM motto this year is:**

"STOP, THINK, CONNECT. Cyber Security is a shared Responsibility"

**The kitchen and laundry are already on the Internet.**

The aim of ECSM month is to raise awareness of network and information security among users and encourage them to acquire knowledge and skills how to avoid and respond to such attacks [https://www.enisa.europa.eu](https://www.enisa.europa.eu). These issues have become increasingly important. At the IFA (Internationale Funk Ausstellung) in Berlin [http://b2b.ifa-berlin.com/](http://b2b.ifa-berlin.com/) manufacturers show a new generation of household appliances that are all connected to the Internet. Therefore security issues have entered the kitchen and laundry room. If the security is not in order, the pot on the stove can suddenly begin to boil over, washing machine will continue to wash and wash endlessly and an empty refrigerator claims to be full. Information technology is penetrating all aspects of our lives calling for security not only for desktop and laptop but also for all household devices.

**Why people have little interest in security?**

At a security conference I attended last year one speaker claimed that only 10% of users would be interested in network and information security. Why is such a low percentage? The reason could be that the internet has been oversold? Today Internet is taken for granted just as electricity and hot water. People generally do not have to worry about the security of electricity and water. If the electricity goes out for a while then there is flashlight or candle somewhere in a drawer. No worries. The same is with hot water. If there is no hot water for a while people just stay inside and put on some extra clothes. No worries. And here is where the overselling starts. People have been told internet is a utility just like electricity and water. No worries. But the Internet has two sides, a personal one and a criminal one.

The visible first side analogous to electricity and water, disconnection is inconvenient, but people accept it as normal. If people are out of touch for
some time people just chat together instead of surfing the Internet. Is this the answer to why 90% of users have no interest in network and information security? They accept that it's okay just like electricity and water, just another utility. With ECSM ENISA wants to change this attitude. "Cyber Security is a shared Responsibility" states that the network and information security is everyone’s concern, not just a few specialists but all. The aim of the month is to reach out to everyone, especially to those 90% of users not interested in network and information security. This is about 450 million people in the EU and EEA. An ambitious task. Emphasis is placed on computer literacy, knowledge sharing and how to best ensure network and information safety.

**Invisible second side of the Internet.** The other side of the Internet is what is happening when everything seems in pretty good order. The question is what is going on behind the scenes not visible and users have no idea of? There can individual criminals and powerful criminal organizations lying in wait to pursue their activities. They get the usernames and passwords they then use themselves or sell. They are also good at getting information out of people by sending the e-mail under a false name and asking for information. Or they sneak into the computer system and lie in wait there. The user does not notice anything while hackers collect information to sell them on. This poses a serious threat to infrastructures provided by companies and public authorities. Many of these infrastructures are vital and a manipulation can cause disasters and life-threatening conditions. Among those are hospitals and power generating stations. But still there are relatively few people or 10% concerned with the issue of network and information security. Almost daily media report about burglaries that provoke fear and anxiety in users, both individuals and companies. No one knows when it will be his or her turn. There are examples of international disputes that have resulted in large-scale cyberattacks. The digital single market will not be realized as long as this is going on. **Lost trust and confidence has to be rebuilt.**

**Politicians have failed too long to understand the importance of the issue.**

Politicians and administrations by nature are not proactive, they are reactive after the fact. For too long, governments did nothing or little to solve the problem. Looked at computer attacks being some sort of youngsters prank. CECUA has long campaigned for computer attack being a crime like any other crime and should be treated as such, with the investigation, prosecution and court. Some have said that cyberspace is completely different and calls for new legislation. CECUA has responded that everything you need to do is to interpret the legislation in modern terms. Everything else is a poor excuse for inaction. Fortunately, this time is behind. And
politicians are catching up however slowly. An old Chinese proverb says that no one will be a good doctor unless you have been sick himself. It could be rewritten in modern terms to say that for somebody to fight cybercrime, he or she must have been victims themselves. It did not take the German parliament long to approve new cyber security law after the parliament had been attacked.

**New thinking in legislation against computer attacks in Europe.**

The legislation extends to those who run the so-called essential infrastructures that are important to society as a whole. It refers to energy, telecommunications, transport, health care, water supply, food production companies, financial institutions and insurance companies that are important for the whole community. These companies have to comply with special obligations:

- Establishing a security system based on the latest technology
- Demonstrate that security systems have been set up.
- Submit the results of network and information security auditing listing weaknesses identified during the auditing.
- Report all attacks they suffer.
- Penalties are up to 100 000 Euros.


The EU is preparing similar legislation.

It is believed that the loss to German companies due to computer crime is several billion Euros a year. Computer crime has become so lucrative that the Mafia finds itself making more money from computer crime than from drugs and prostitution combined. Other new opportunity is that insurance companies are starting to offer insurance against losses due to cyberattacks. It is not a question of if, but only when companies suffer damage. The insurance companies see a new and an attractive market.

**Slow reacting politicians.**

This was a step long overdue. CECUA commented extensively on the strategy. A quote:

“The strategy uses down to earth terminology: online or offline. Those are terms everybody can understand. Furthermore, it aligns the online and the offline: same fundamental rights, democracy and rule of law. And the offline has jurisdiction over the online. Same laws apply. And no new laws are needed”. For details see www.cecuarchives.eu

And a quote from CECUA’s yearly report for 2014:

“In 2013 the Commission finally turned its attention to security issues and published Cyber Security Strategy for the European Union. This document is a good step in the right direction. CECUA has already commented on the strategy on its website www.cecua.eu However, the Strategy is really a draft of what is needed. Fraud in Cyber Space has reached such dimension that it has become a real malice resulting in threats for users, society, general infrastructure and economic production. And the Commission is still only groping with the issue slowly accepting that Cyber-crime is a crime and has to be dealt with as such. This includes reporting the crime, something the Commission is still hesitant about. The strategy is also hesitant on user issues. Yes, the Commission acknowledges that the users need somebody to turn to if they have problems. But who? The Commission leaves it open” For full report see www.cecua.eu

When it comes to the end-users the Cybersecurity strategy is a bit short. Searching the document for “user” delivers only one hit:

“The Commission invites the Member States to: Organize a yearly cyber-security month with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users.”

Now we are back to the ECSM organized by ENISA. It is a huge task reaching out to potentially 450 million people. ENISA has chosen a practical approach of organizing the ECM month in cooperation with partners in the member states. The partners or multipliers know the local conditions and ENISA provides the infrastructure and overall organization. Not all member states participate but quite a few do.

This was the only mentioned action with reference to end users and it is up to the Member States to carry it out. Is one month enough? Definitely not. We need 12 cyber-security months, many cyber-security years to raise enough awareness to be successful. And who is to organize it and who is to finance it? ENISA has taken on a huge task with very limited resources.
"STOP, THINK, CONNECT. Cyber Security is a shared Responsibility"

The aim of ECSM month is to raise awareness of network and information security among users and encourage them to acquire knowledge and skills how to avoid and respond to such attacks https://www.enisa.europa.eu

To acquire knowledge and skills or so called e-skills is certainly a good approach. But how will the 450 million people acquire those skills? Does this call for reformation of the education system to teach e-skills in all schools? But still it will take a whole generation until the 450 million have acquired those e-skills. Of course, we do not need 450 million computer experts. But we need people aware of the danger and possessing knowhow to avoid it. Therefore, the ECSM is only a start, an early start on a long journey.

CECUA is happy to be a ECSM partner and will use its experience and expertise and network to promote the issue.

Prof. Dr. Jon Thorhallsson
President CECUA

jon.thorhallsson@cecu.eu