Fighting cybercrime

As the online part of our lives is increasing, through the use of home banking or shopping online, so is organised crime in the cyber environment. Today, cybercriminals steal bank and credit card details to sell onwards for as little as €1 per card or €60 per bank credentials. Cybercrime is a profitable activity that traverses borders, but involves little risk. It is a problem that affects all of us and that we need to tackle together.

What is cybercrime?
Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a problem that knows no borders and that can take on different forms. Yet, all these forms have two characteristics in common: they can be committed on a mass-scale and a great geographical distance can lie between the location of the criminal and the effects of the crime.

In the narrower sense, cybercrime includes online fraud and forgery. Large-scale fraud can be committed through various instruments, such as identity theft, phishing (attempts to acquire sensitive information, such as passwords and credit card details, by pretending to be a trustworthy person), spam and malicious code (computer viruses).

The publication of illegal content online is another form of cybercrime. Such content includes child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia. These are considered criminal acts in many but not all countries.

Yet another form includes attacks against information systems, denial of service attacks and hacking. Information systems are often attacked through botnets, which consist of a “herd” of computers that have been infected with a virus (“zombies” or “bots”, short for robots) and that, unbeknownst to their owners, are under the control of another computer.

Whom does cybercrime affect?
Nobody is safe from cybercrime. It affects citizens, businesses, governments and critical infrastructures alike.

Every day, there are more than one million cybercrime victims worldwide. People can become victims of theft of account and credit card details via e-mails that appear to come from their banks. They may fall prey to fake online...
shops or have their smartphones hacked into. Social media is another target; for example, up to 600,000 Facebook accounts are compromised daily.

Cyber attacks against critical infrastructures can have far-reaching effects on businesses, governments and even on societies. For example, the use of malware or botnets for large-scale attacks against information and communication technology (ICT) infrastructures can disrupt the provision of vital goods or services. These kinds of attacks can also disrupt the maintenance of other critical infrastructures, such as transport or energy networks.

What is the EU response to cybercrime?

As a low risk-high reward activity, cybercrime has become a wide-spread, borderless problem. Therefore, collaboration at EU level is essential to fight it.

The EU focuses on improving operational cooperation between law enforcement authorities and coordination between EU States, including on awareness-raising, training and research activities. It also facilitates dialogue with industry, which controls a large part of information infrastructures.

Several EU legislative actions also contribute to the fight against cybercrime. These include the:

- 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences;
- 2002 ePiracy Directive, whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information;
- 2005 Framework Decision on attacks against information systems, and the Directive proposed in 2010 to replace it, which aims at better addressing large-scale simultaneous attacks and botnets;
- 2011 Directive on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse).

The European Network and Information Security Agency assists EU States in addressing, responding to and preventing information security problems, and promotes public-private cooperation. A European Cybercrime Centre has also been proposed to serve as the focal point for information, pool expertise in support of EU States’ capacity building and support EU States’ investigations. The Centre will warn EU States of major cybercrime threats on the horizon and alert them to weaknesses in their online defences. In addition, it will map criminal activities by identifying patterns in, for example, virus attacks, keeping both authorities and citizens informed of any new developments.

For more information about what the European Union does to fight cybercrime, visit our website: [ec.europa.eu/home-affairs](http://ec.europa.eu/home-affairs)