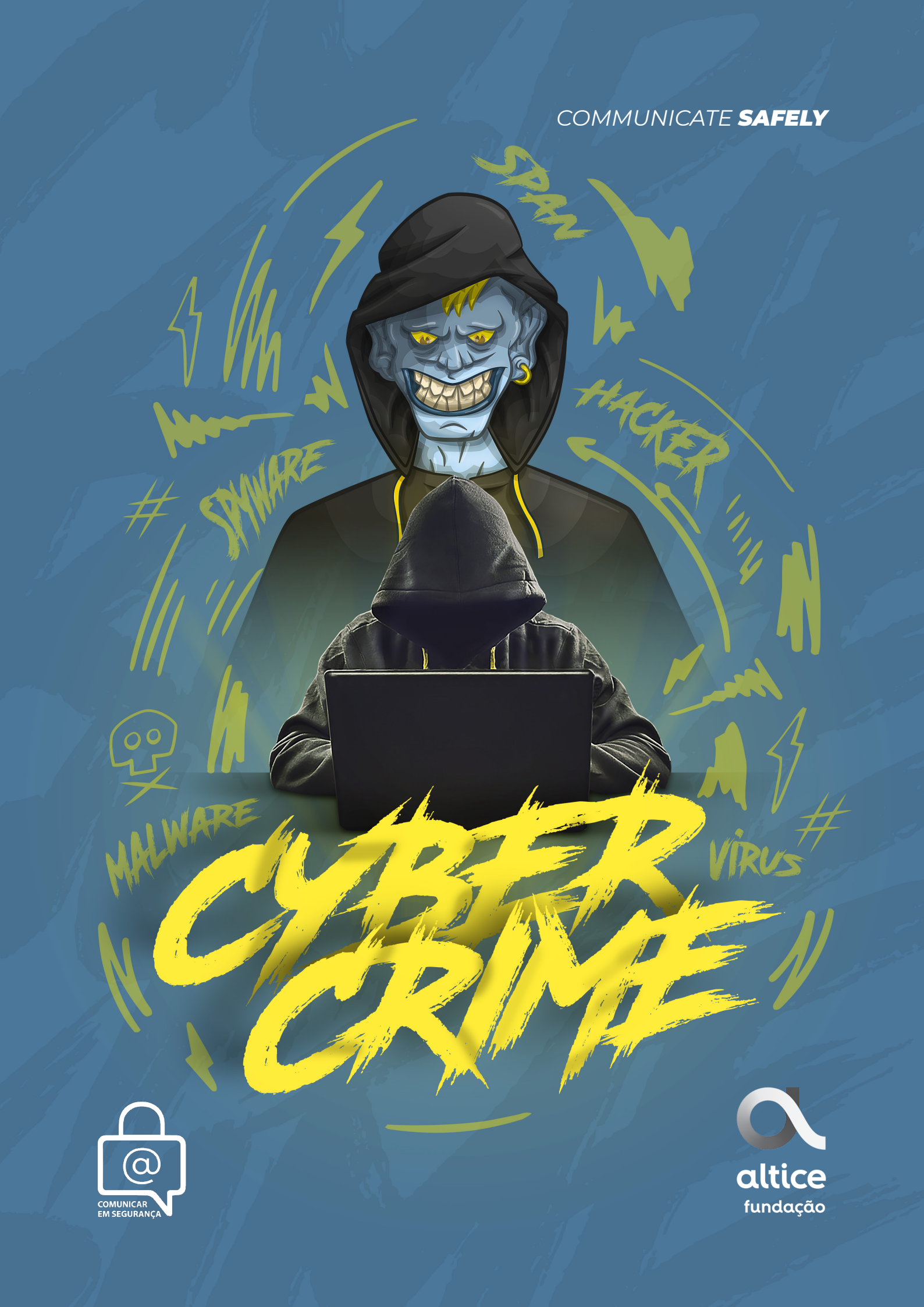
COMMUNICATE **SAFELY**



COMUNICAR EM SEGURANÇA

altice fundação

RANSOMWARE

PHISHING

ONLINE SCAMS

CREATING FAKE PROFILES

STEALING PERSONAL PROFILES

CYBERBULLYING

AFTER ALL, IT DOESN'T HAPPEN ONLY TO OTHERS...

AND NOW, WHAT DO I DO?

WHAT IS IT?

Cybercrime is the name given to any illicit and illegal practice carried out digitally. These crimes are aimed at technological equipment (computers, tablets, mobile phones, etc.) and networks, carried out through the Internet. If there were no Internet, these crimes would not exist.

Cybercrime includes several practices, such as stealing personal data, installing viruses and malware, creating fake profiles on the Internet (for example on social networks or to carry out fraud schemes), online scams or cyberbullying.

One of the major difficulties in fighting cybercrime is its transnational nature. In many situations, it is very difficult to identify the origin of the crime and its perpetrators. A person may be the victim of a cybercrime committed in a country other than their own, which raises numerous difficulties in fighting this type of crime and applying consequent punishment. Each country has its own legal framework for cybercrime, and often there is no punishment or laws for cybercrime.

Due to the increasing use of the Internet and technological equipment, it is essential for users to have knowledge about Technology, Networks and Cybersecurity in order to be able to protect themselves and avoid these situations.

Many situations of online scams, fraud schemes and stealing personal data can be avoided with more conscious and preventive behaviours. Many cybercriminals “take advantage” of users’ lack of knowledge and imprudence to commit crimes. However, the victims of this type of crime can be both individuals and companies.

TYPES OF CYBER CRIME

RANSOMWARE

It is a type of malware (malicious programme) that causes the operating system and equipment to block until the ransom is paid. The ransom is always virtual and usually occurs by using a virtual currency, called bitcoin. This crime is committed by sending phishing emails or fake websites, using Social Engineering.

STEALING PERSONAL DATA

Stealing confidential personal information such as credit card details, bank details, email accounts in order to later sell it or use it for illicit acts. This crime is often carried out using Social Engineering or sending targeted emails to obtain people's data.

STALKING AND REVENGE PORN

Online relationships can lead to cybercrime situations. In this type of relationships, people share their personal data such as photos, videos, emails or passwords and may subsequently become victims of this type of crime.

Sharing intimate photos and videos (sexting) can lead to cases of revenge porn and sextortion, that is, the unauthorised sharing of intimate photos and videos, and threats. It is a very common situation at the end of personal relationships. Stalking people online through technological means is also considered a crime. Attackers may be known or unknown to the victim, and it is an extremely intrusive crime.

ONLINE SCAMS

Online scams can have a financial or personal/romance motivation. There are the simple e-commerce scams such as an online purchase where the good is never received although payment has been made, or websites that manage to store users' bank details.
Bank scams are often originated by sending phishing emails. Users believe they are accessing their bank, and give their access (login and password) to the criminals.

Romance scams occur when the criminal manages to establish a personal and trusting relationship with the victim and then commits financial extortion and fraud.

CYBERBULLYING

Cyberbullying can be seen as a form or extension of bullying that is carried out through digital media. It is also aggressive, intentional and ongoing behaviour. It can happen anywhere, anytime, constantly.

The aggressor is often anonymous, there is physical distance, aggressions arrive through mobile phones, social networks and messages, thus contributing to the complexity of the phenomenon and to the worsening of the emotional consequences for the victims.

HINTS/ SUGGESTIONS

Watch out for suspicious e-mails:
Check the origin/sender of the email; Check for spelling errors; Watch out for links or attachments.

Online shopping:
Do some research about the credibility and security of the website (ex: https, padlock); Use a secure payment system (Paypal, Multibanco, MBnet, cash on delivery).

Antivirus and Firewall
installed and updated.

Having strong and different
passwords for every website.

Making regular backups
to avoid losing information.

Using secure Wi-Fi or VPN networks.

Keeping software up-to-date.

Keeping personal data and information private or blocked on Social Networks.
Social Engineering uses this type of data.

Not accepting contacts from unknown people.

Not sharing photos or videos with strangers.

Not sending intimate photos or videos
that can be used for sextortion/revenge porn.

In Cyberbullying situations, it is essential to ask for help.

Keeping emails and messages
that can be used as evidence.

AÇOR LARANJA

WE ALL HAVE AN OBLIGATION TO DO OUR PART AGAINST CYBERCRIME.

ASK FOR HELP! REPORT DENOUNCE!

ONLINE **SAFETY HELPLINE**

800 21 90 90

PROJECT

COMUNICAR EM SEGURANÇA

SPONSOR

altice fundação

FUNDING PARTNER

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

Centro Internet Segura