CRIF CYBER OBSERVATORY

2022

The CRIF Cyber Observatory analyzes the vulnerability of people and companies to cyber-attacks, interprets the main trends concerning data exchange on the web, and offers suggestions for mitigating cyber risk.

A STUDY THAT GOES DEEP, EXPLORING BOTH THE OPEN AND DARK WEB ENVIRONMENTS.

OPEN WEB

Indexed by search engines. Accessible to everyone via the most popular browsers

DARK WEB

Hidden, not indexed by search engines. Accessible via encrypted navigation software to guarantee anonymity.

THE IDEAL PLACE FOR HACKERS AND CYBERCRIMINAL ACTIVITIES

RECORD OF PERSONAL DATA CIRCULATING ON THE DARK WEB

MORE THAN 1.6 MILLION CRIF CYBER ALERTS

1

Users alerted

about cyber-attacks against their personal data

Stolen information can be used for a variety of purposes, such as to break into victims’ accounts, misuse services, extort or steal money or engage in scams such as phishing or smishing.

83.7%

in relation to data found on the

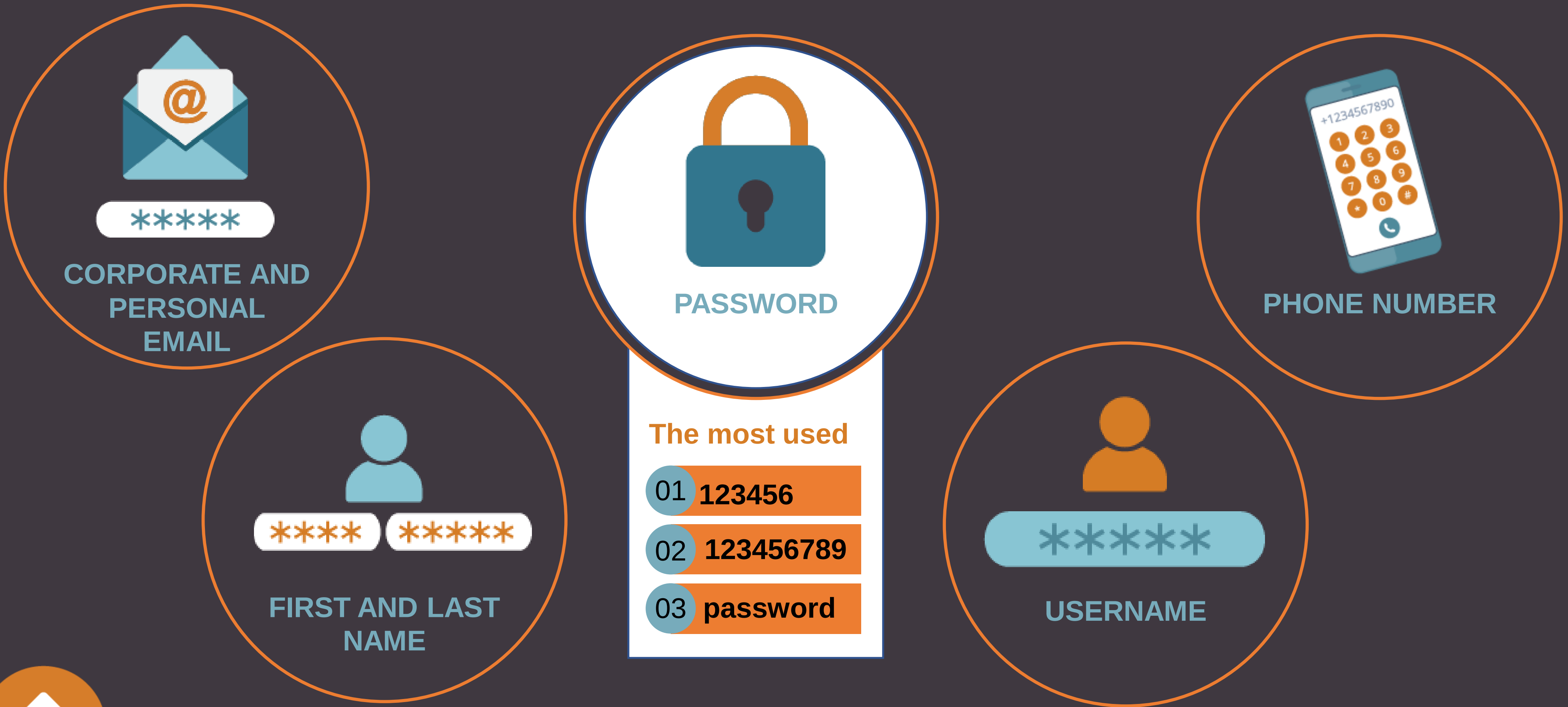
DARK WEB

16.3%

in relation to data found on the

OPEN WEB

The most vulnerable data on the web



CORPORATE AND PERSONAL EMAIL

PASSWORD

The most used

01 123456

02 123456789

03 password

PHONE NUMBER

FIRST AND LAST NAME

USERNAME

Passwords and emails are confirmed to be the most vulnerable data along with phone numbers, and are valuable data for accessing many platforms and apps with 2-factor authentication login procedures.

CRIF Together to the next level

The most intercepted data combinations

+10.5%

+ CVV and expiry date

FULL CREDIT CARD WITH FIRST AND LAST NAME

98.1%

PHONE NUMBER + FIRST AND LAST NAME

49.2%

EMAIL + PASSWORD

90.5%

PHONE NUMBER + PASSWORD

13.2%

*****

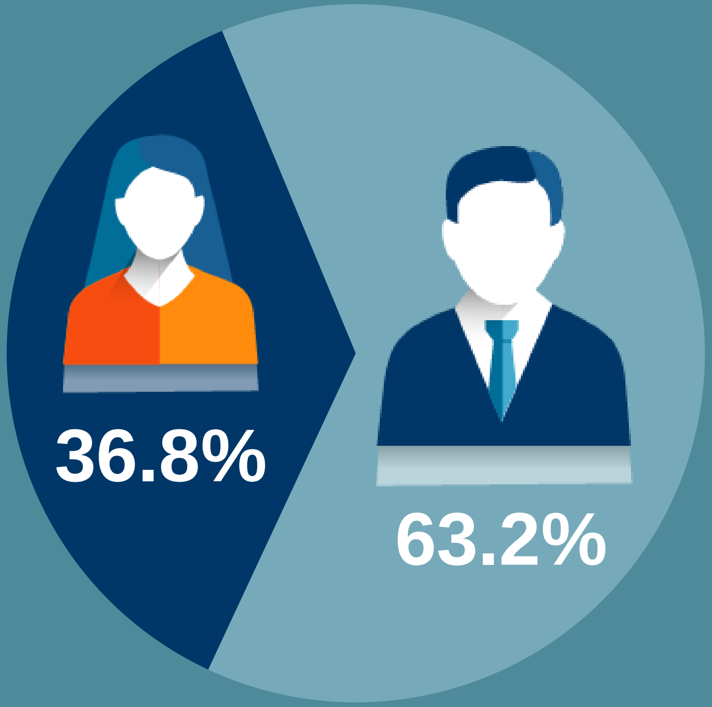
USERNAME + PASSWORD

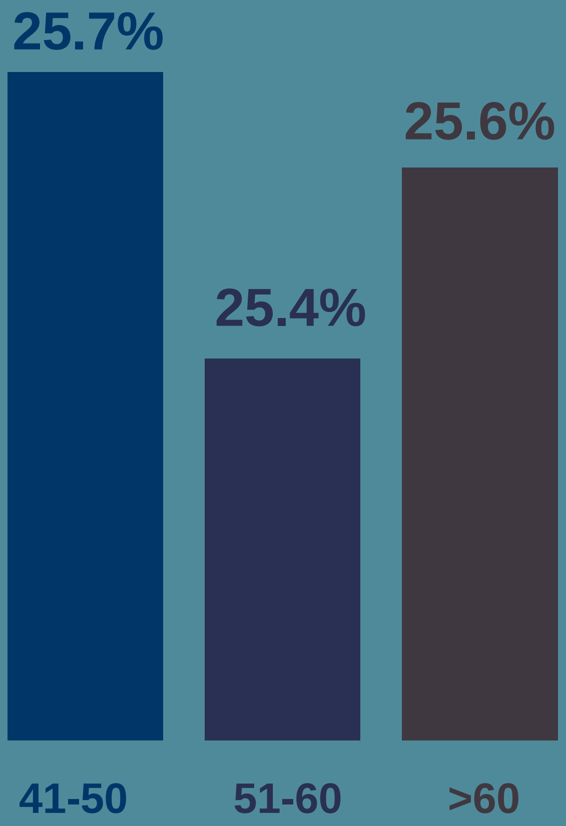
71.7%

The increased interception of combined credit card number, CVV and expiry date (+ 10.5%) is of a particular concern. Through these credentials, hackers can steal money or complete transactions on the open web and dark web.

* 2022 vs 2021 change

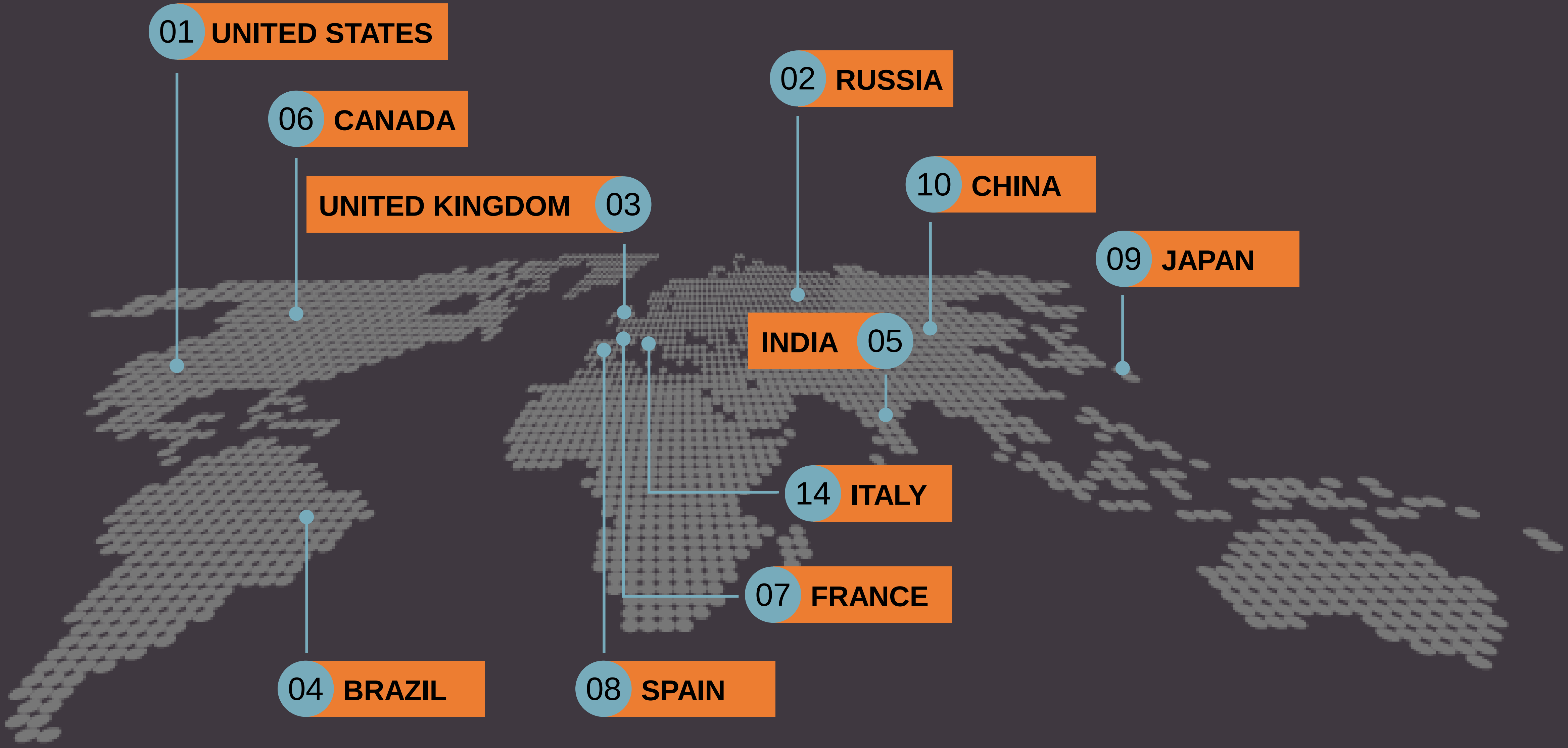
Profile of the most affected users





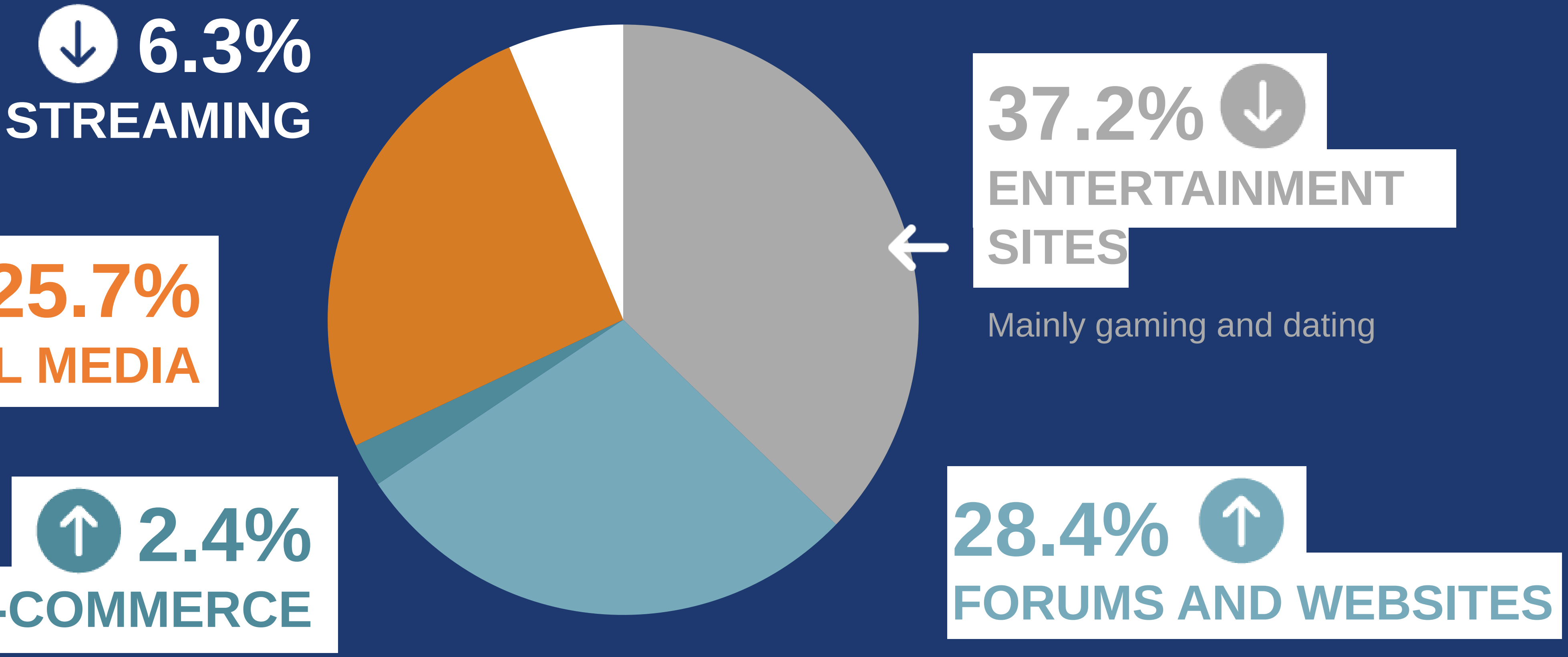
The age groups most affected are men over 40. The under 30s are less at risk, probably thanks to their greater familiarity with digital environments.

Where credit card data is stolen the most



CRIF
Together to the next level

Most stolen account types



Entertainment site accounts are the most stolen, especially online gaming and dating accounts. However, the most significant increase concerns the theft of social media accounts, such as Facebook, Twitter, Instagram and LinkedIn, which can lead to fraud and identity theft.

The latest edition of the CRIF Cyber Observatory confirms the significance of our data to fraudsters.
In fact, the circulation of data in 2022 was much higher than in the past, so much so that **data found on the dark web tripled compared to the previous year**. The reasons for this increase relate to the current geopolitical situation, which is seeing intense activity not only on the "physical" battlefields but also on the virtual battlefield, the so-called "**cyberwar**”.
The danger of a phishing attacks or data theft
is always lurking. CRIF aims to
increase awareness about phishing among both young people and adults alike, promoting cyber educational initiatives, such as the **Cyberninja game**.

Beatrice Rubini, CRIF Executive Director

SAFE BROWSING

Tips to protect yourself against identity theft and digital fraud

Choose secure passwords
It is important to choose long and different passwords for each account, using combinations unrelated to personal information.

Install antivirus software and keep your software updated
To constantly improve the security of your devices it is essential to keep them updated and protected.

Back up your data
Make regular full backups to avoid data loss. In addition, make a copy of your documents (at the very least the most important or most used ones) so that they are always recoverable via the internet.

Protect your devices
Set up a screen lock with PIN, password, fingerprint or facial recognition, and turn on remote control for remote locking. Prevent others from using them without your consent. Set up monitoring.

Beware of suspicious messages, emails and phone calls
Always be wary of any attempt at contact that requires the provision of personal or financial information.

Use monitoring services
Choosing specific solutions to monitor the circulation of your data on the web is the best strategy for more comprehensive protection.

For more information:
marketing@crif.com