CRIF CYBER OBSERVATORY

2023

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

OVER 7,5 BILLION OF DATA CIRCULATING ON THE DARK WEB

NEARLY 1.9 MILLION CRIF CYBER ALERTS

+13.9% 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**.

77.5%

in relation to data found on the

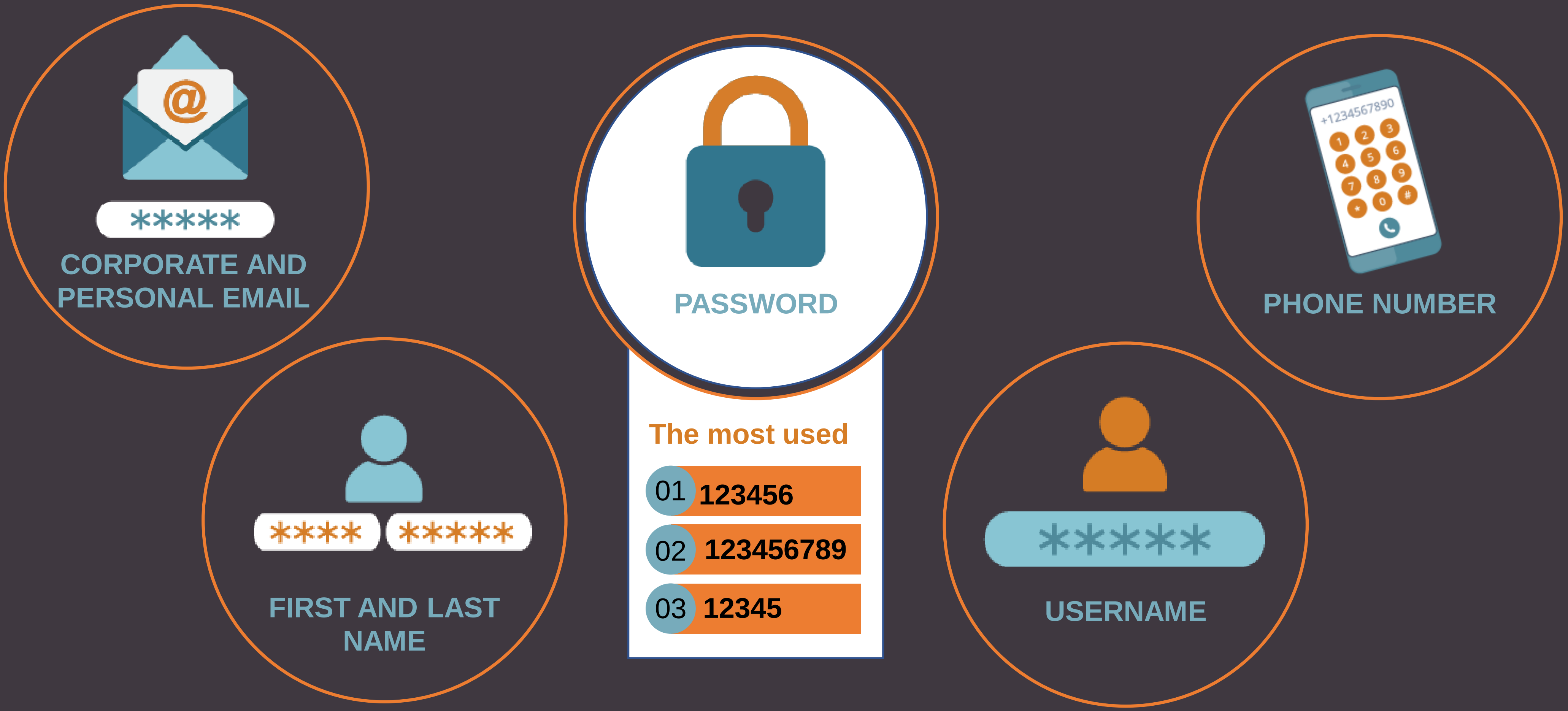
DARK WEB

22.5%

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	**12345**

PHONE NUMBER

FIRST AND LAST NAME

USERNAME

The most intercepted data combinations

+ CVV and expiry date

FULL CREDIT CARD WITH CVV AND EXPIRY DATE

96.9%

PHONE NUMBER + FIRST AND LAST NAME

38.7%

PHONE NUMBER + PASSWORD

16.6%

+25.6%

USERNAME + PASSWORD

65.6%

EMAIL + PASSWORD

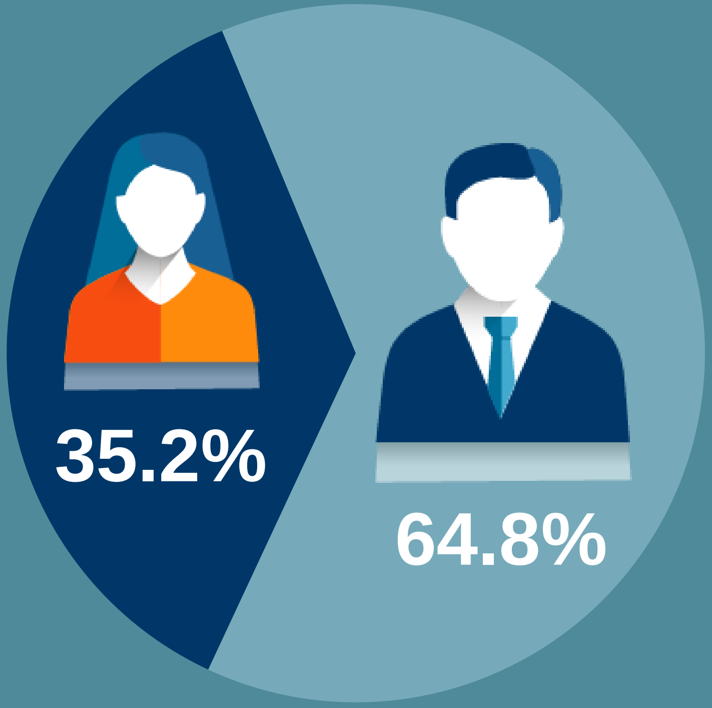
94.4%

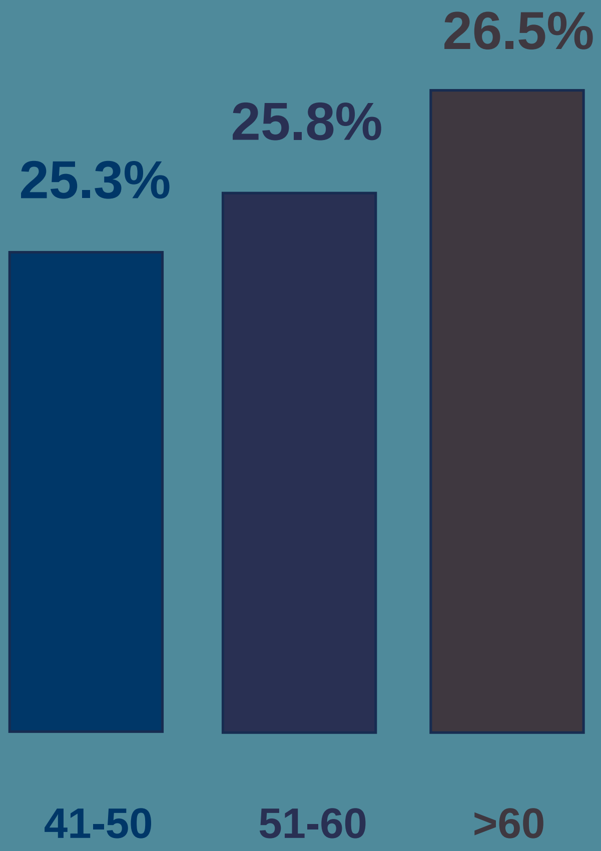
The increased interception of combined phone number and password (+ 25.6%) is of a particular concern as it increases the vulnerability of the victim.

*** 2023 vs 2022 change**

CRIF Together to the next level

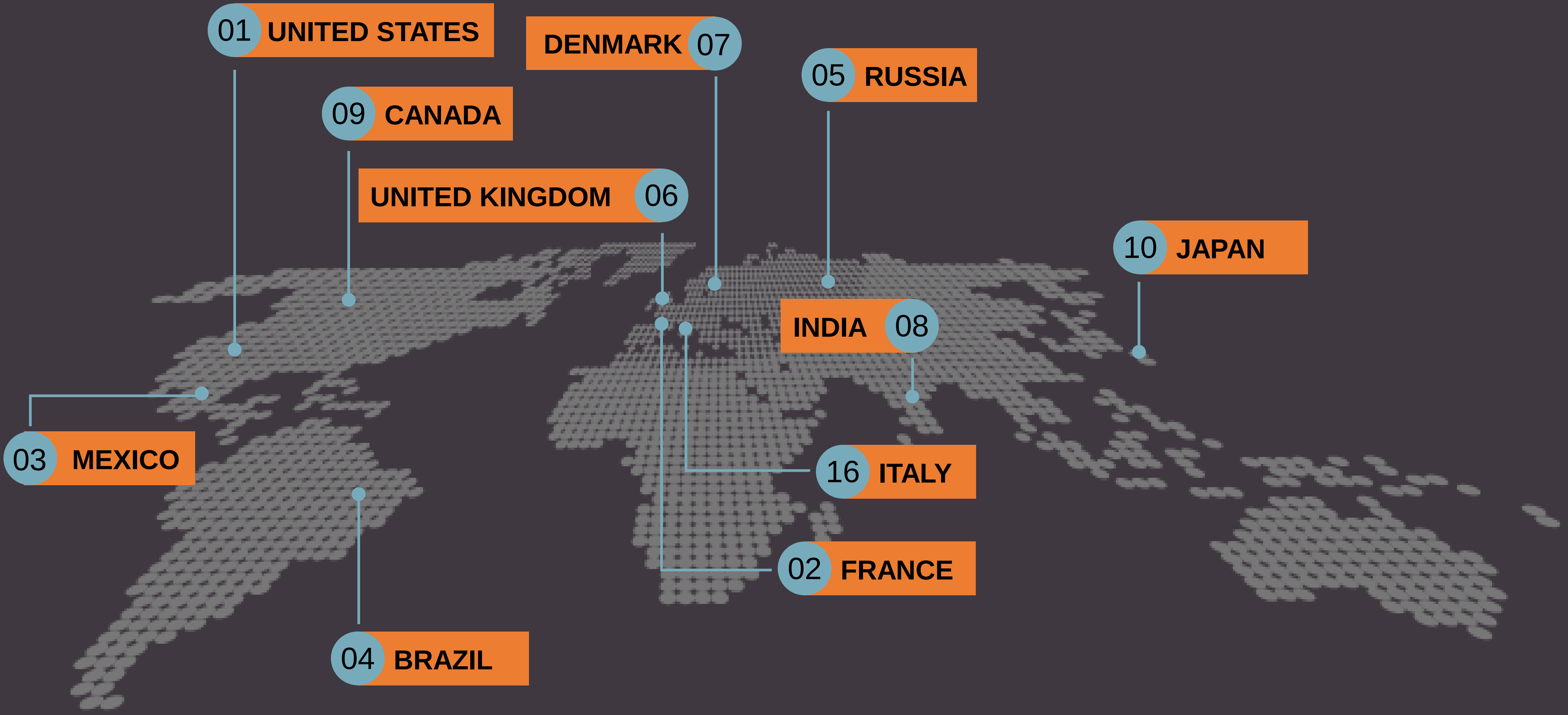
Profile of the most affected users





The age groups most affected are those over 60 years old, followed by 51-60 and 41-50 years old.

Where credit card data is stolen the most

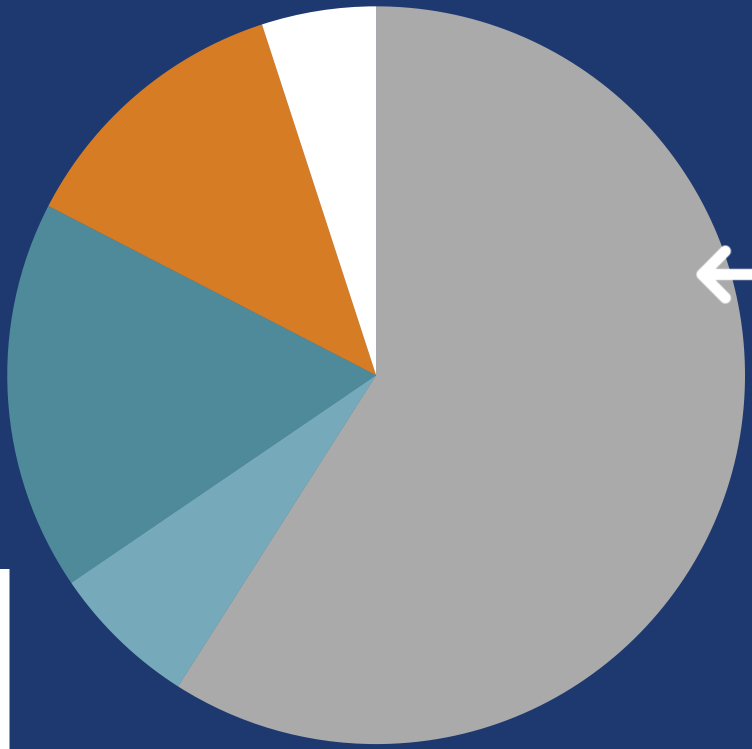


Most stolen account types

↑ 4.8%
FINANCIAL SERVICES

↓ 11.9%
SOCIAL MEDIA

↑ 16.4%
E-COMMERCE



56.6% ↑
ENTERTAINMENT SITES

Mainly gaming and dating

6.2% ↓
FORUMS AND WEBSITES

↑

Entertainment site accounts are the most stolen, especially online gaming and dating accounts, followed by e-commerce and social media accounts. The risk of theft of such accounts can lead to direct economic consequences for victims and has increased compared to last year.

> There are some trends to keep in mind about cyber risk: for personal data theft, cybercriminals use malware and applications that over time have become increasingly sophisticated and difficult to distinguish from official ones, becoming a trap for people. Moreover, cybercriminals who use Artificial Intelligence to target consumers are becoming a real threat due to increasingly sophisticated email scams, characterized by correct and therefore plausible language, and the ever-evolving code generation for malicious app generation.
> We need to pay particular attention to the emails and messages we receive every day, training ourselves to recognize scams and phishing attempts. It is advisable for consumers to manage their data scrupulously, also relying on tools that today allow us to protect devices and monitor our data.

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