Cyber Observatory

CRIF-Mister Credit

2024

CRIF

Together to the next level

The phenomenon and the most “desirable” data

2.1 MILLION

cyber alerts by CRIF

88%

users alerted for data found on the **dark web**

and

12%

users alerted for data found on the **open web**

+15.4 alerts related data exposure on the dark web

MOST VULNERABLE DATA ON THE WEB

PASSWORDS

the most used:

123456

123456789

12345678

Passwords and email addresses remain the most vulnerable data, along with **usernames,** followed by phone numbers and full names.

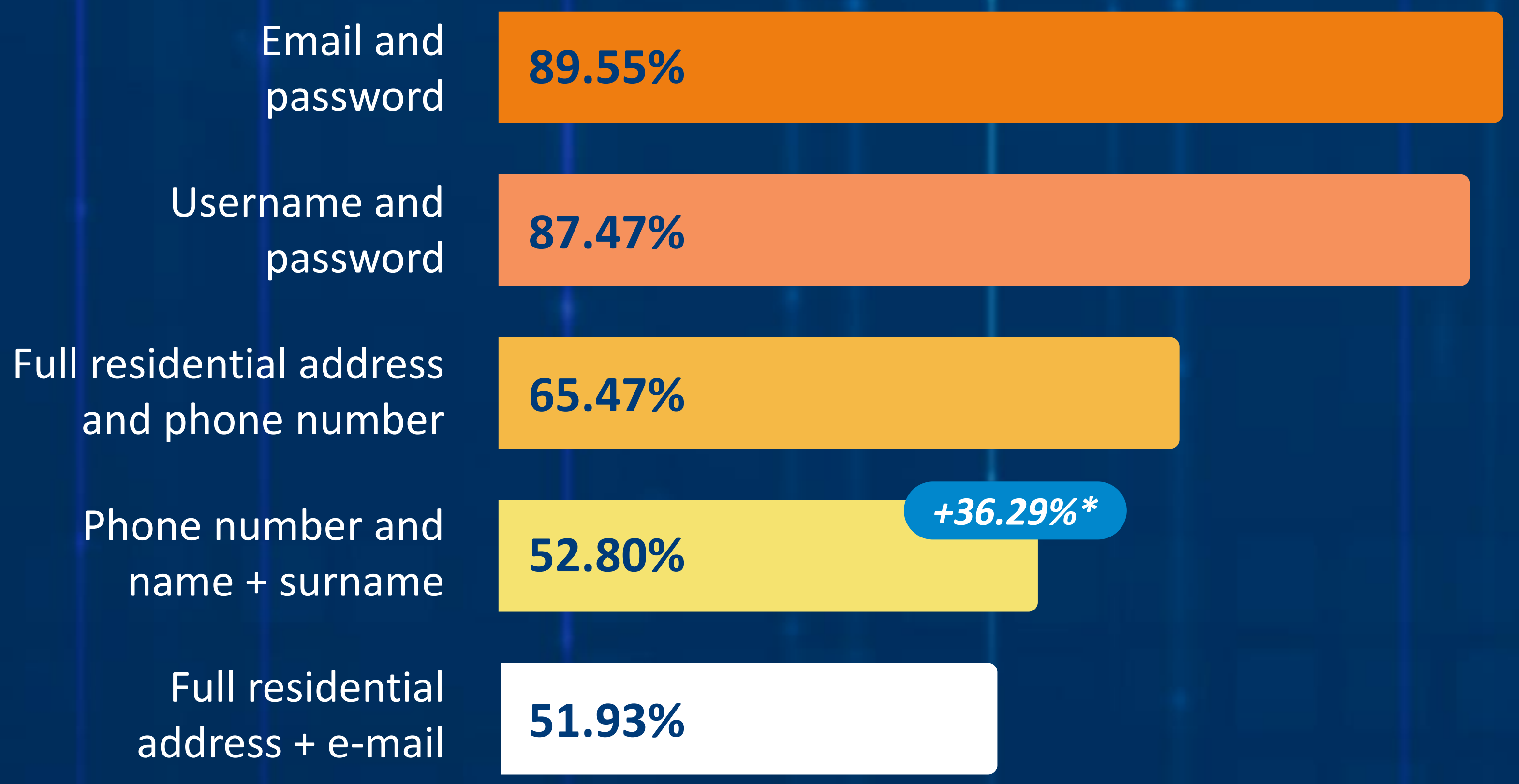
Personal and business e-mail

Phone number

Name and surname

Username

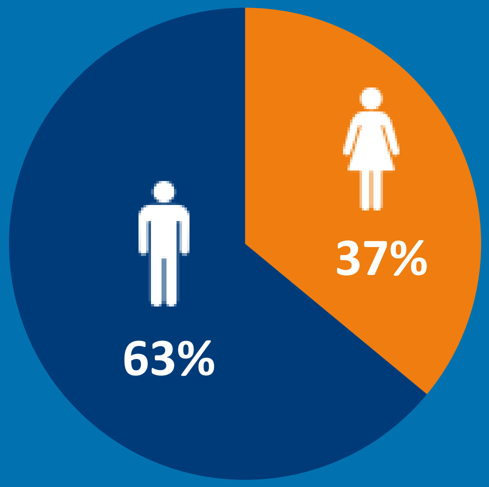
MOST EXPOSED DATA COMBINATIONS

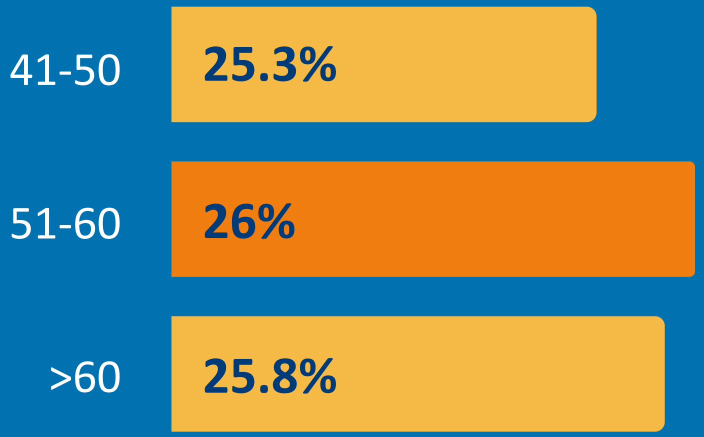


The increase of +36.29% compared to the previous semester regarding the combination of **phone number, name and surname in relevant.** This type of combination increases the victim's vulnerability.

*change 2024 vs 2023

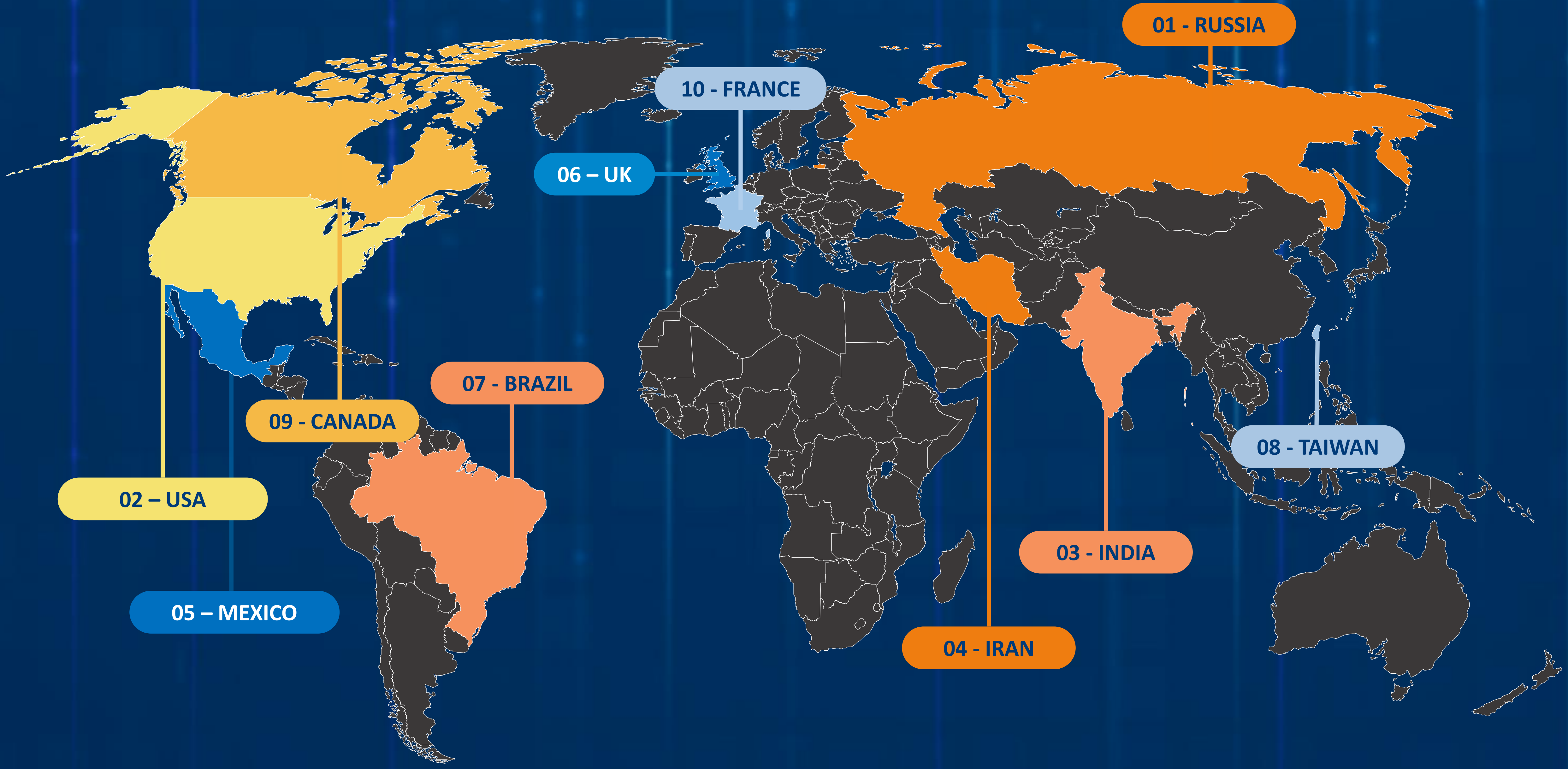
PROFILE OF THE MOST AFFECTED USERS



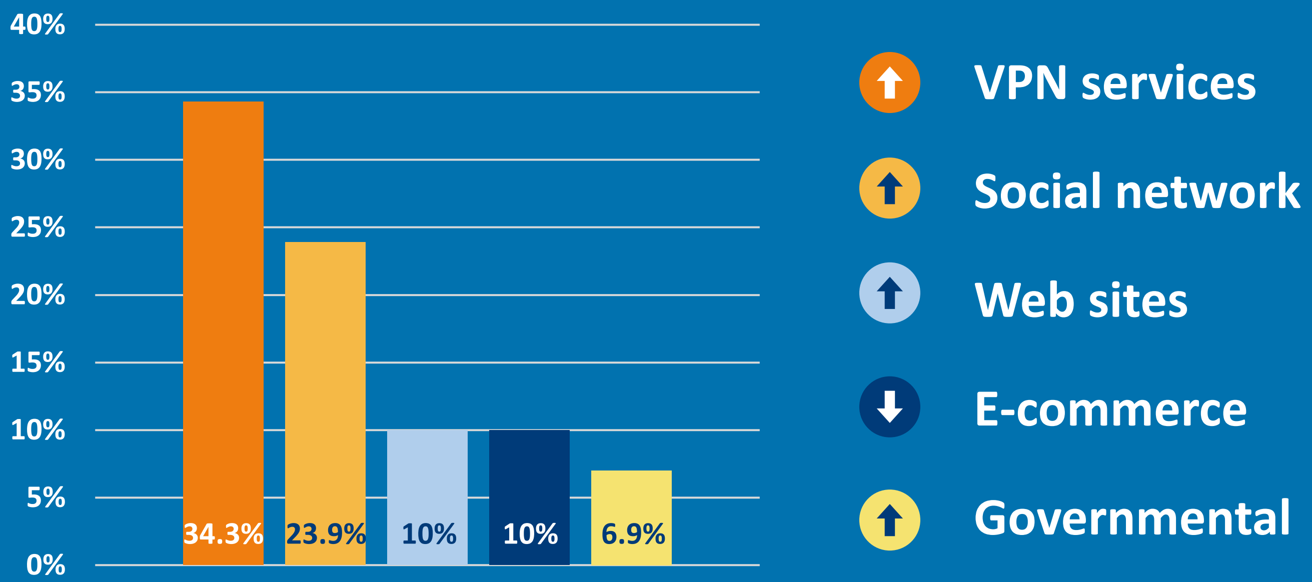


The age group most affected is **51-60** years old, followed by the **over 60** years old and those **41-50** years old.

WHERE CREDIT CARD DATA IS STOLEN THE MOST



MOST STOLEN ACCOUNT TYPES EXCLUDING EMAIL SERVICES



Excluding email services, most stolen accounts are associated with **VPN services, social network accounts, websites, and e-commerce.**

The risk of theft of these accounts can lead to **direct economic consequences** for the victims.

“

Not only must we pay attention to the data we share and protect it with appropriate tools, but it is also essential to be aware of new attack techniques and the vulnerabilities of the systems and devices we use daily.

The rapid evolution of advanced AI, while providing benefits like conversational chatbots, has significantly increased social engineering threats. As online content become more and more AI-generated new challenges arise for many users who are unaware of the power and ease with which these technologies can be deployed by scammers.

As CRIF, we provide several initiatives to inform users of the evolving risks, encouraging them to stay cautious in their online activities in order to safeguard their personal data.

The lack of awareness is precisely what malicious actors exploit.

Moreover, global geopolitical tensions, combined with the evolution of cybercriminal techniques thanks to AI, make even more necessary to adopt preventive protection measures and proactive reactions against potential attacks targeting, business, critical infrastructures and government institutions.

”

Beatrice Rubini – CRIF Executive Director

The Cyber Observatory aims to analyse the vulnerabilities of individuals and organisations to cyber-attacks and to interpret emerging trends related to data exchanged in **OPEN WEB** and **DARK WEB environments.**

It examines the types of information, the sectors where data traffic is concentrated, and the countries most exposed.

PUBLIC WEB

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

DARK WEB

Hidden, accessible only through specific browsers or targeted searches. Accessible via encrypted navigation software to guarantee anonymity.

THE IDEAL PLACE FOR HACKERS AND CYBERCRIMINALS ACTIVITIES

TIPS TO PROTECT YOURSELF FROM IDENTITY THEFT AND DIGITAL SCAMS

Choose secure passwords: it is important to choose long and different passwords for each account, using combinations unrelated to personal informations.

Enable automatic updates for your operating system, applications, and browser To ensure your device is always protected against the latest threats and vulnerabilities that cybercrime may exploit.

Regularly back up your data to the cloud or external devices and periodically check the integrity of these backups. Additionally, make copies of your documents, especially the most important or frequently used ones, so that they are always recoverable online.

Protect your devices: use PINs, passwords, facial recognition, and two-factor authentication for an extra layer of security. Additionally, enable remote control and data wipe features in case of loss or theft.

Be wary of suspicious websites, e-mails, and calls: always verify the authenticity of websites by checking their URL and security certificate. Avoid clicking on suspicious links in SMS, WhatsApp messages, or e-mails. Never provide personal or financial information via messages or phone calls.

For Comprehensive Security, use services to monitor the circulation of your personal and financial data online and employ robust antivirus protection on your devices.