Cyber Observatory

CRIF-Mister Credit

2025

Together to the next level

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

The phenomenon and the most “desirable” data

2.2 MILLION

cyber alerts by CRIF

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

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

+5.8 alerts related data exposure on the dark web

MOST VULNERABLE DATA ON THE WEB

PASSWORDS

the most used:

123456

123456789

12345678

2. E-MAIL

Personal and business

*Increase in compromised business accounts (from **8,7%** to **9,8%**)*

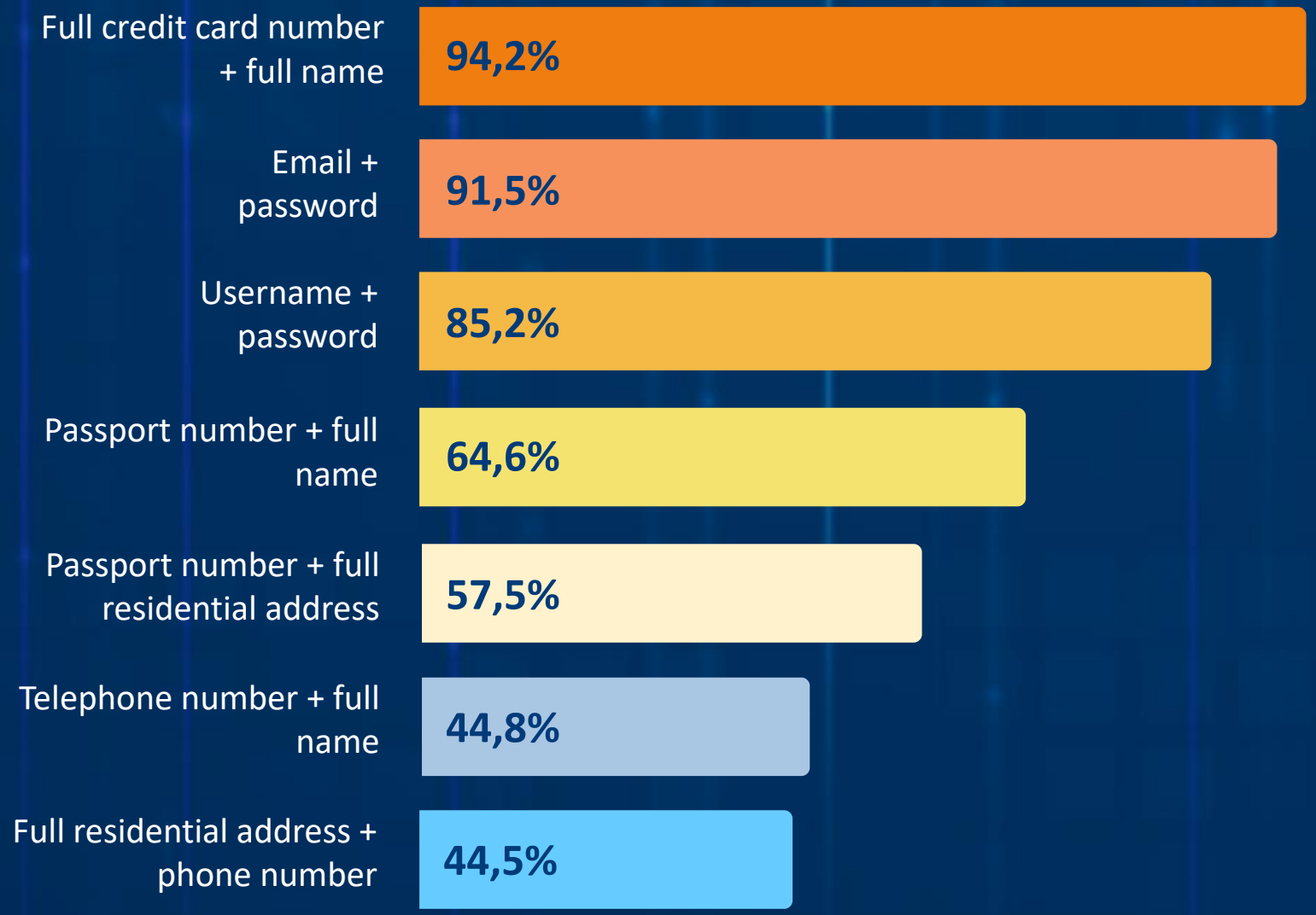
3. Username

4. Full residential address

5. Name and surname

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

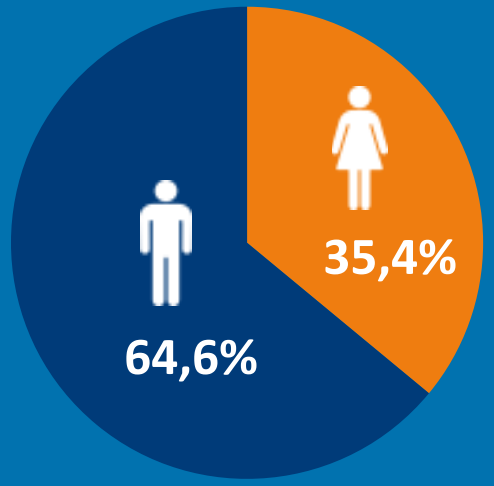
MOST EXPOSED DATA COMBINATIONS

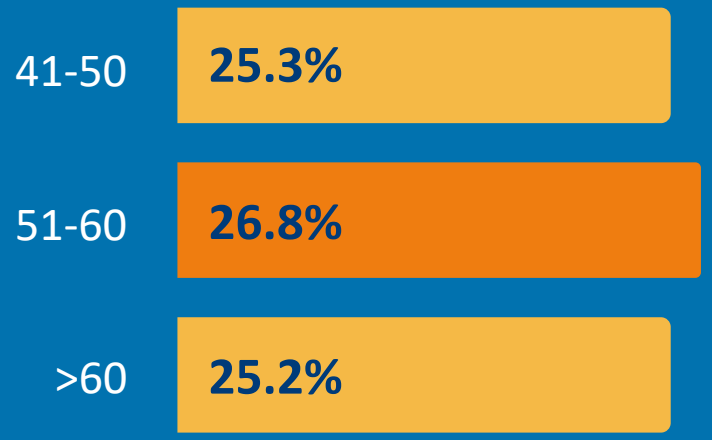


Of particular concern is the combination of credit card numbers and full name, found in 94.20% of cases.

Significantly increased compared to 2024, it is highly alarming due to the serious risk of financial fraud.

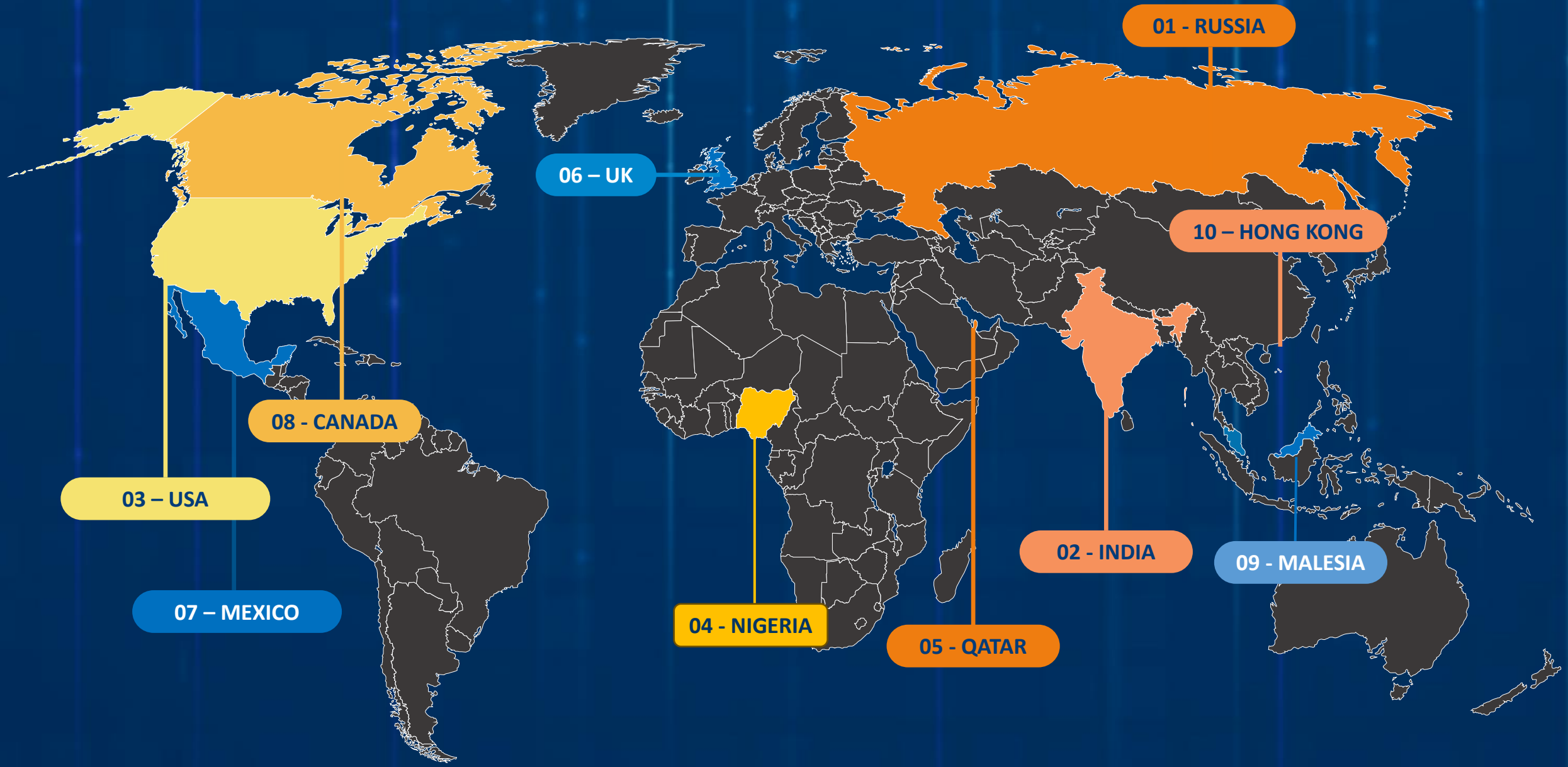
PROFILE OF THE MOST AFFECTED USERS



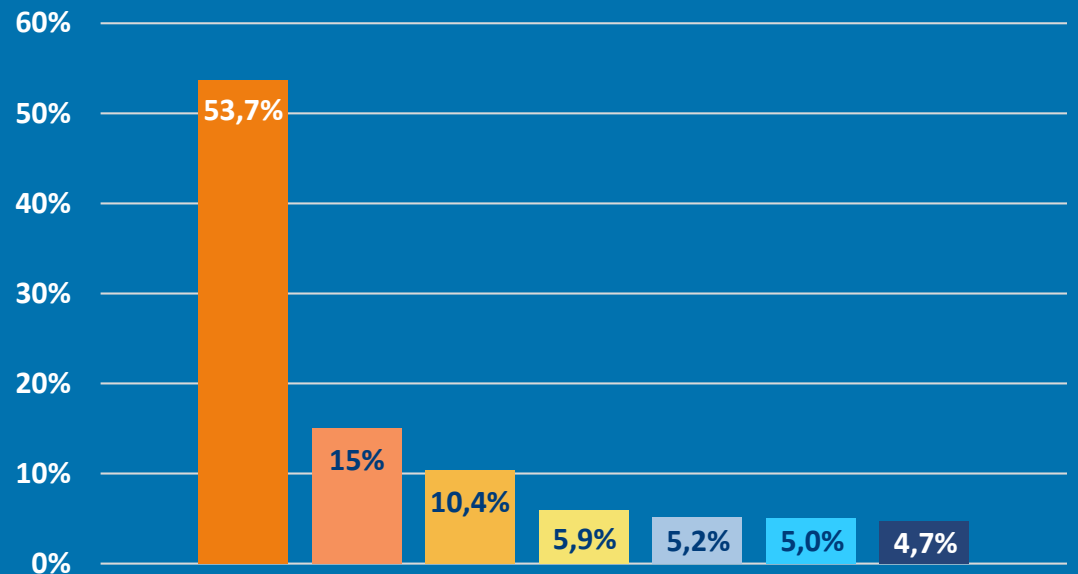


The age group most affected is **51-60** years old, followed by those **41-50** years old and the **over 60** years old.

WHERE CREDIT CARD DATA IS STOLEN THE MOST



MOST STOLEN ACCOUNT TYPES EXCLUDING EMAIL SERVICES



- **VPN Services**
- **Social network**
- **Web sites**
- **Gaming**
- **Governmental**
- **E-commerce platforms**
- **Financial services**

Excluding email services, most stolen accounts are associated with **VPN services, social network accounts, websites, and gaming.** The risk of theft of these accounts can lead to **direct economic consequences** for the victims.

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.

The cyber threats landscape is rapidly and constantly evolving. In 2025 we saw the rise of new technologies and actors, with phishing attacks upgraded by AI and hyper-personalized content deceiving victims with unprecedented precision. Furthermore, identity-based attacks are ever more common, with aggressors exploiting compromised credentials to access critical systems. However, 2025 has also highlighted another front: ***companies are becoming increasingly exposed and attractive targets****. Wealthier data combinations circulate in the dark web, including personal information, as well as professional credentials and references to business accounts. These datasets allow precise attacks against business processes and operative platforms, turning every compromised credential into a potential entry point to the organization's systems.*

Protecting our data and paying attention to what we share remains essential, but it is not enough: today it is fundamental to identify the new attack techniques made possible by Artificial Intelligence, such as e-mails generated by advanced language models, deepfake audio and video, convincing multi-channel phishing campaigns.

In a context characterized by geopolitical tensions and increasingly automated cyber-attacks, preventive safety measures and rapid responses are essential to protect people, companies, critical infrastructures and institutions from targeted threats. As CRIF, we continue educating users on these evolving dangers, encouraging them to safeguard their personal data and keep updated on new kinds of online scams, since lack of awareness is still the most exploited element by attackers.

Beatrice Rubini – CRIF Executive Director