

Following yesterday's announcement of CARNET's national CERT on the leakage of data on 226 million unique user accounts, of which over 47,000 are accounts with e-mail addresses ending in .hr (eg name.surname@domena.hr), the Agency for the protection of personal data wants to draw the attention of all citizens of the Republic of Croatia to the importance of establishing appropriate technical measures for personal data protection on online services they use (eg social networks, web shops, etc.), or setting appropriate strong passwords.

The Agency's recommendation is that users create a separate strong password for each login to the Internet service or other service they use to access that service or service, and not to use the same username and password for multiple services or services.

A strong security password contains:

- 16 or more characters (the more the better),
- capital letters (ABCDEFGH...),
- lowercase letters (abcdefgh ()),
- figures (34 123456),
- symbols (@ # \$% {} [] () / \ " ' , ; : . < > ...).

We also advise citizens to, in accordance with the instructions of the national CERT on the service "Have I Been Pwned" via the link <https://haveibeenpwned.com/> check ALL their email addresses that they use as a username to log in to Internet services or services (not only those that end in .hr) are compromised, ie are in hacker databases. If they find that a particular email address has been compromised, we suggest the following:

- As a precaution, change the password for this email address to a new strong security password
- in all Internet services and Internet services in which they used that e-mail address as a login user name (eg social networks, Internet shop, etc.) create a new separate strong security password for each of these services and services. If this Internet service or service is offered, it would be advisable to include the double authentication option.