Major IR leaks – The Cyber Shafarat – Membership only site

cybershafarat.com/2024/09/04/major-ir-leaks/

September 4, 2024

LEAKFA

Currently includes:
48 major leaks
10 minor leaks
for a total of 58 leaks

Source and statement

This page only shows leaks over 5k lines. Minor leaks are only available for victim inquiries.

The magnitude of the leak, exposed items and affected accounts are obtained after removing duplicates and incorrect items and may differ from the original data.

The information sources of this website are taken from available and public databases on the Internet, the website does not save the original information of the databases, only the things needed for users' searches are stored in coded form. Attacking this website does not provide you with any information. This website will take legal action if any intrusion attempt is detected.

Major leaks

National Bank of IranThe magnitude of the leak69,900,000confirmedgeneralimportant

Disclosed items

Name, surname, father's name, date of birth, national number, card number, mobile phone number, city, province, address

narration

In 1400, a database containing the information of more than 70 million real and legal customers of the National Bank of Iran was put up for sale on dark web markets. A few days later, a part of this database was published in a hacker forum. This data included first name, last name, father's name, date of birth, national number and other information of customers. In an announcement, National Bank Public Relations, while emphasizing the use of information security equipment, controls, policies and procedures based on standards and methods and upstream requirements, denied the published claims regarding the leakage of customer information and added, "Currently, the investigations are also continues, but no results have been obtained regarding the validity of this claim".

Leak date: 12 January 1400
Affected accounts: 69,976,577
In the news: attached reportExport Bank of IranThe magnitude of the leak63,000,000confirmedgeneral

Disclosed items

Account number, customer number, name, surname, card number, username, internet bank password, password reminder, email address, mobile phone number, account type, account opening date, branch code

narration

In April 2019, a database containing the information of 63 million real and legal customers of Saderat Bank of Iran was put up for sale in one of the hacker forums. family name, account number, customer number, card number, account type, email address and other information. Saderat Bank of Iran has not shown any official reaction to this issue, but Saderat Bank's public relations in a conversation with Mahname Farahed announced that "initial checks of the published information show that this news is not very accurate and they are investigating it more closely."

Leak date: April 19, 2019
Affected accounts: 63,091,551
In the news: Euronews reportInstagramThe magnitude of the leak40,000,000confirmedgeneral

Disclosed items

User ID, Username, Full Name, Email Address, Mobile Number, Profile Picture, Privacy Status, Account Verification Status

narration

In Isfand 1400, security researcher Bob Dyachenko announced the disclosure of the information of millions of Iranian users by an unprotected Elasticsearch. It was made publicly available due to misconfiguration of security settings. A few months later, a database containing information on more than 40 million Instagram accounts and 1.2 million Twitter accounts, including user IDs, usernames, full names, locations, website addresses, profile pictures, profile bios, mobile phone numbers, and email addresses. which was hosted on this website, was put up for sale on a hacker forum.

Leak date: March 4, 1400
Affected accounts: 40,694,833
in the news: Tejaratnews reportIrancellThe magnitude of the leak37,000,000confirmedgeneralimportant

Disclosed items

Name, surname, landline phone number, mobile phone number, city, place of residence, postal code, national number

narration

In June 2014, Irancell, a communication service company that operates Iran's largest mobile phone network, suffered a data failure. This data breach led to the disclosure of its customers' information, including more than 37 million names, surnames, mobile and

landline numbers, provinces, cities, residential addresses, zip codes and national codes. Irancell did not take responsibility for the leak of this data and blamed the competitors for the confusion caused by this news.

Leak date: June 27, 2013
Affected accounts: 37,084,245
Official statement: Irancell statementhunting systemThe magnitude of the leak35,200,000confirmedgeneral

Disclosed items

Full name, username, user ID, profile biography, mobile phone number

narration

In April 2019, Bob Dyachenko, a security researcher, discovered a huge collection of data that was related to Iranians and was placed in an unprotected database. According to him, it took 11 days for this database, which was hosted on a service called “Samaneh Shekar”, to become unavailable, which has caused other people to gain access to it and put the data up for sale. This incident led to the disclosure of the information of 35 million Telegram user accounts, including names, user IDs, usernames, phone numbers, hashes, and secret keys, along with the information of 4 million Instagram user accounts, including usernames, profile pictures, names, and biographies. (Bio) became users.

Leak date: April 2, 2019
Affected accounts: 35,253,119
In the news: ISNA reportMellat BankThe magnitude of the leak30,000,000confirmedgeneralimportant

Disclosed items

Name, surname, father’s name, birth certificate number, national number, date of birth, city, province, city of birth, province of birth, address or address, account number, card number, mobile phone number

narration

In May 1400, a database containing the information of more than 30 million real and legal customers of Bank Mellat was put up for sale in one of the hacker forums. These data include name, surname, father’s name, national ID number, national code, date of birth, city. , province, address and other information of customers. Bank Mellat has not yet taken responsibility for the leakage of this data, and by publishing a notice, while emphasizing the

bank’s commitment to protect the information of its customers, it announced that “the dimensions of this claim are being investigated by the bank’s specialized and technical teams”.

Leak date: May 22, 1400
Affected accounts: 30,099,465
In the news: Mehr reporttraysThe magnitude of the leak26,300,000confirmedgeneralimportant

Disclosed items

Name, Surname, National Number, Date of Birth, Gender, Email Address, Mobile Phone Number, User ID, User Status, Platform Type, Software Market, Software Code Version, Google Advertising ID, Device ID, Device Model, Matrix Session ID, Matrix user ID, city, geographic coordinates, last activity time, trip code, trip status, service type, trip date, trip start time, trip origin and destination, driver ID, driver’s name and surname, driver’s phone number, trip cost, share the traveler

narration

In September 1402, Tapsi, one of the largest active software in the field of Internet taxis, was infiltrated by a group of hackers known as “IRLeaks”. Some time later, Tapsy’s CEO announced on Twitter that “Hackers have accessed some of Tapsy’s users’ information and were looking for extortion, but Tapsy has decided not to cooperate with them.” This decision, however, did not prevent the disclosure of user information, and finally the data was put up for sale in dark web markets. This data contained the personal and identity information of more than 26 million passengers and 3 million Tapsi drivers, along with travel information and the source code of all products such as passenger and ambassador software, development, support, back-end and other departments. Until now, Tapsi has not taken responsibility for the leakage of this data and has not published any official announcement in this regard.

Leak date: September 11, 1402
Affected accounts: 26,334,060
In the news: Tejaratnews reportTelegramThe magnitude of the leak21,000,000confirmedgeneral

Disclosed items

Name, surname, username, user ID, mobile phone number

narration

In May 2019, Telegram, a multi-platform open source messaging service focused on privacy, suffered a data breach. The report of this incident was first published by the Russian website active in the field of technology “Kod.ru”. According to this report, a database was put up for sale on the dark web markets, which contains the data of more than 30 million Telegram user accounts (21 million Iranians and 12 million Russians) included names, usernames, user IDs and mobile phone numbers. The approximate simultaneity of this event with the “Hunting System” data leak led to this news being interpreted and not covered in the Persian language media.

Leak date: May 6, 2019
Affected accounts: 21,056,273
In the news: Medusa reportTraffic police – license plateThe magnitude of the leak11,000,000confirmedgeneralimportant

Disclosed items

First name, last name, father’s name, national number, birth certificate number, date of birth, mobile phone number, landline number, address, car license plate number, car class, car brand, car type, car color, car body number, number Engine serial, manufacturer, year of manufacture, VIN number, type, date and description of court orders issued for the vehicle

narration

In July 1400, a database containing about 14 million lines of information on the owners of all types of vehicles that were registered by the traffic police until the end of 2019 was put up for sale in a hacker forum. Rahor Police did not react to this incident at first, but about a month after the publication of this news, Colonel Hossein Ramezani, Executive Deputy of Rahor Naja Police, while rejecting the published news regarding the disclosure of information, stated: “So far, not even one bit of this information It has not been published and this issue is only an allegation.” Unfortunately, a total of 11,033,390 license plates of personal vehicles, government offices and institutions, taxis, public vehicles, agricultural machinery, disabled and veterans, and 2,621,698 motorcycle license plates were affected by this data leak. , last name, father’s name, birth certificate number, national number, date of birth, mobile phone number, address, license plate number, manufacturer, year of manufacture and other information of the owners of active license plates in Iran.

Leak date: July 31, 1400
Affected accounts: 11,033,390
In the news: Rukna reportQalamchi CenterThe magnitude of the leak4,300,000confirmedimportant

Disclosed items

First name, last name, father’s name, national number, gender, date of birth, numerator, test group, field location, field address, representative name, backup, director’s name, exam contact number, school name, registration date, landline phone number, Cell phone number, supervisor’s cell phone number, province, city, address, grade point average, first and second semester average balance, average exam balance, number of registration exams, absentee and attended summer and normal

narration

On the 1400th day, one of the servers of the “Education Cultural Center”. Qalam Chi” was hacked by an unknown person. A few days later, a database containing more than 6 million lines of personal information, registrations and tests of students in the collection was put up for sale on a hacker forum. These data included name, surname, father’s name, national number, gender, date of birth and other information of students. Kalamchi Education Cultural Center has not taken responsibility for the leakage of this data and only warned the students about changing their password every two weeks by sending a short message.

Date of leak: 9 January 1400
Affected accounts: 4,328,721Badsaba call to prayer calendarThe magnitude of the leak4,200,000confirmed

Disclosed items

Name, surname, father’s name, user ID, email address, country, province, city, time zone, geographic coordinates, mobile phone number, device brand, device model, IMEI ID, software code version, Android version, registration date, Comments and suggestions, tracking code

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident eventually led to the disclosure of various information from the employees and users of Badsaba call to prayer calendar software, Mufatih al-Jinan audio Bab al-Naim, Habal al-Matin audio Quran, Nahj al-Balagheh audio chemistry, better score educational software, Parsman Islamic software, and Shia Rooz Shamar software. And several other services/software became “mobile wave pioneers” that are available for victim inquiries.

Leak date: January 24, 2019
Affected accounts: 4,279,930Driver’s trayThe magnitude of the leak3,600,000confirmedgeneralimportant

Disclosed items

Name, Surname, National Number, Date of Birth, Gender, Email Address, Mobile Phone Number, User ID, User Status, Platform Type, Software Market, Software Code Version, Google Advertising ID, Device ID, Device Model, Matrix Session ID, Metrics user ID, city, geographic coordinates, last activity time

narration

In September 1402, Tapsi, one of the largest active software in the field of Internet taxis, was infiltrated by a group of hackers known as “IRLeaks”. Some time later, Tapsy’s CEO announced on Twitter that “Hackers have accessed some of Tapsy’s users’ information and were looking for extortion, but Tapsy has decided not to cooperate with them.” This decision, however, did not prevent the disclosure of user information, and finally the data was put up for sale in dark web markets. This data contained the personal and identity information of more than 26 million passengers and 3 million Tapsi drivers, along with travel information and the source code of all products such as passenger and ambassador software, development, support, back-end and other departments. Until now, Tapsi has not taken responsibility for the leakage of this data and has not published any official announcement in this regard.

Leak date: September 11, 1402
Affected accounts: 3,666,198
In the news: Tejaratnews reportAudio Qur’an of Habal al-MateenThe magnitude of the leak2,800,000confirmed

Disclosed items

Full name, username, user ID, password, city, email address, mobile phone number, device brand, device model, IMEI ID, Wi-Fi mac address, software code version, software serial, Android version, Android ID, Tertiles, registration date Name, Internet connection status

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident finally led to the disclosure of about 2 million and 900 thousand lines of name, username, password, city, email address, mobile phone number, mobile phone brand, mobile phone model, IMEI ID, Wi-Fi MAC address and other information of “Quran” software users. “Habal El Matin Audio” and several other services/software became “Mobile Wave Pioneers Company”.

Leak date: January 24, 2019
Affected accounts: 2,856,963Traffic Police – Engine license plateThe magnitude of the leak2,600,000confirmedgeneralimportant

Disclosed items

Name, surname, father's name, national number, date of birth, mobile phone number, landline number, address, motorcycle license plate number, motorcycle brand, motorcycle type, motorcycle color, motorcycle body number, engine serial number, manufacturer , year of manufacture, VIN number, type, date and description of court orders issued for the motorcycle

narration

In July 1400, a database containing about 14 million lines of information on the owners of all types of vehicles that were registered by the traffic police until the end of 2019 was put up for sale in a hacker forum. Rahor Police did not react to this incident at first, but about a month after the publication of this news, Colonel Hossein Ramezani, Executive Deputy of Rahor Naja Police, while rejecting the published news regarding the disclosure of information, stated: "So far, not even one bit of this information It has not been published and this issue is only an allegation." Unfortunately, a total of 11,033,390 license plates of personal vehicles, government offices and institutions, taxis, public vehicles, agricultural machinery, disabled and veterans, and 2,621,698 motorcycle license plates were affected by this data leak. , last name, father's name, birth certificate number, national number, date of birth, mobile phone number, address, license plate number, manufacturer, year of manufacture and other information of the owners of active license plates in Iran.

Leak date: July 31, 1400
Affected accounts: 2,621,698
In the news: Rokna reportAudio Mufatih Bab Al-NaimThe magnitude of the leak2,100,000confirmed

Disclosed items

Full name, username, user ID, password, city, email address, mobile phone number, device brand, device model, IMEI ID, Wi-Fi mac address, software code version, software serial, Android version, Android ID, Tertiles, registration date Name, Internet connection status

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by

infiltrating the server of one software. This incident finally led to the disclosure of about 2 million and 200 thousand lines of name, username, password, city, email address, mobile phone number, mobile phone brand, mobile phone model, IMEI ID, Wi-Fi MAC address and other information of Mofatih software users. “Bob Al-Naim Audio” and several other services/software became “Mobile Wave Pioneers Company”.

Leak date: January 24, 2019
Affected accounts: 2,176,234Judiciary – case management systemThe magnitude of the leak1,900,000confirmedgeneralimportant

Disclosed items

Name, surname, father’s name, national number, birth certificate number, educational qualification, religion, gender, date of birth, address or address, mobile phone number, landline number, email address, personal password number, file number, file title, type Case, case subject, case summary, case status, case charge, case code number, registration date, confidentiality status, investigative branch, registering unit, assembly report, text of assembly report, date of meeting, penalty request, letters

narration

In March 1402, the judiciary’s case management system was infiltrated by a group of hackers known as “Adalat Ali”. A few days later, hackers made the data extracted from this system available to the public on a website. This action caused the personal and identity information of millions of Iranian citizens whose information was registered in this system to be exposed and put at risk. The reaction of the Judiciary, like the previous leaks, was denial. A well-informed judicial official, whose name is usually not published, in a conversation with Isna, denied the issue of hacking the judiciary’s systems and said: “Many of these documents are fake and fictitious and even old administrative letters that were previously published in cyberspace and Reposted again.” At the request of users, Likfa is currently hosting the latest version of the data for this leak. If the site is updated, new data will be checked and added.

Leak date: March 1, 1402
Affected accounts: 1,197,241
In the news: Zomit reportFacebookThe magnitude of the leak1,600,000confirmedgeneral

Disclosed items

Name, surname, gender, date of birth, user ID, mobile phone number, email address, place of birth, place of residence, marital status, employment status, registration date, date of obtaining the last degree.

narration

In June 2019, a database containing the information of more than 530 million Facebook users from all over the world was put up for sale in a hacker forum. This data, which contained the information of 1.6 million Iranian users, includes name, surname, gender, date of birth, user ID, mobile phone number, email address, place of birth, place of residence, marital status, employment status, and registration date. The name and date of obtaining the last academic degree. Facebook announced that the source of extracting this information was a vulnerability that was fixed in August 2018.

Leak date: June 17, 2019
Affected accounts: 1,685,080
In the news: Verge reportRaichtThe magnitude of the leak1,200,000confirmedgeneral

Disclosed items

Full name, email address, mobile phone number, password, IP address, profile picture, geographic coordinates, user browser details, last visited page

narration

In February 2019, Bob Dyachenko, a security researcher, discovered a huge collection of data related to the online chat platform “Raichat” and was placed in an unprotected database. The registration of this database in the search engines of devices connected to the Internet made it accessible to other people. A few months later, a database containing more than 150 million lines of data including names, email addresses, mobile phone numbers, passwords, profile pictures, IP addresses and other information of the website’s users was put up for sale on a hacker forum.

Leak date: February 9, 2019
Affected accounts: 1,268,558
Official statement: Raicht’s statementTwitterThe magnitude of the leak1,200,000confirmedgeneral

Disclosed items

User ID, Username, Full Name, Location, Website Address, Profile Picture, Profile Biography, Mobile Number, Email Address

narration

In Isfand 1400, security researcher Bob Dyachenko announced the disclosure of the information of millions of Iranian users by an unprotected Elasticsearch. It was made publicly available due to misconfiguration of security settings. A few months later, a database containing the information of 1.2 million Twitter accounts and more than 40 million Instagram

accounts including user ID, username, full name, email address, mobile phone number, profile picture, privacy status and account verification status (Verified Badge) of users, which was hosted on this website, was put up for sale in one of the hacker forums.

Leak date: March 4, 1400
Affected accounts: 1,214,286
In the news: Tejaratnews reportPunishaThe magnitude of the leak786,000confirmedgeneralimportant

Disclosed items

Name, Surname, Gender, National Number, Date of Birth, Username, User ID, Mobile Number, City, Country, Address or Address, Subscription Type, Profile Image, Cover Image, Projects, Contests, Website Address, Skills work portfolio, resume, fluent languages, work history, education history, achievements, marital status, time zone, last time of activity

narration

In July 2019, the freelancer recruitment service or online project “Punisha” was leaked due to the misconfiguration of Elasticsearch. A few months later, a database containing the information of more than 270,000 users of this website was put up for sale on a hacker forum. This information included name, surname, gender, national number, date of birth, username, mobile phone number, city, country, account type and other user information. Two years later, on February 28, 1401, this site suffered a data leak again in the same way. This time, however, the information included about 800,000 users, along with the data related to competitions and projects. But the new CEO Punisha attributed the reason for this new leak to the hacker attack and said, “The amount of sensitive information leaked is less than a tenth of this (announced) amount.”

Leak date: July 1, 2019
Affected accounts: 786,202
In the news: Attached report
Read more: Punisha and multiple leaksMinistry of Cooperation – Tehran Labor DepartmentThe magnitude of the leak598,000confirmedimportant

Disclosed items

User ID, username, password, first name, last name, father’s name, birth certificate number, national number, gender, date of birth, education level, email address, mobile phone number, landline number, city, area code, address or address , zip code, personnel code, workplace, IP address, last entry date

narration

In December 2019, a database containing more than 630 thousand lines of information related to the “General Department of Cooperative, Labor and Social Welfare of Tehran Province” was put up for sale in one of the hacker forums. The data included name, surname, national code, date of birth, gender, personnel code, educational qualification, email address, address, postal code and other information of users/employees of the Ministry of Cooperatives, Labor and Social Welfare. Unfortunately, no reaction has been shown from the Ministry of Home Affairs or the relevant news agencies regarding this information leak. The data was provided to Leakfa by a source who asked to be identified as “Sm0rfZ”.

Leak date: January 11, 2019
Affected accounts: 598,157RoseblogThe magnitude of the leak288,000confirmed

Disclosed items

Full name, username, password, email address, IP address, website address

narration

In December 2012, Roseblog, one of the providers of web writing services (blog) in Persian language, was hacked by an unknown person. A few months later, the database of this site containing the information of more than 280 thousand users, including names, usernames, passwords, email addresses and IP addresses of users, was published among hacker forums and groups.

Leak date: January 11, 2012
Affected accounts: 288,585Smalayo educational systemThe magnitude of the leak238,000confirmedimportant

Disclosed items

User ID, username, password, first name, last name, national number, date of birth, gender, email address, mobile phone number, year of study, credits obtained, study center

narration

In July 1401, the comprehensive educational system of Samalayo suffered a data leak due to the misconfiguration of security settings. A few days later, a database containing the information of more than 200,000 users of this website was put up for sale on a hacker forum, and some time later it was released to the public. This information included name, surname, national number, date of birth, gender, email address, mobile phone number and other information of the students.

Leak date: July 5, 1401
Affected accounts: 238,807Nahj al-Balagha audio chemistryThe magnitude of the

leak224,000confirmed

Disclosed items

Full name, username, user ID, password, city, email address, mobile phone number, device brand, device model, IMEI ID, Wi-Fi mac address, software code version, software serial, Android version, Android ID, Tertiles, registration date Name, Internet connection status

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident finally led to the disclosure of about 225,000 lines of name, username, password, city, email address, mobile phone number, mobile phone brand, mobile phone model, IMEI ID, Wi-Fi MAC address and other information of the users of “Nahj Balaghah Audio Kimia” software. ” and several other services/software became “mobile pioneer company”.

Leak date: January 24, 2019
Affected accounts: 224,234Ministry of Interior – Seman SystemThe magnitude of the leak126,000confirmedimportant

Disclosed items

Name, surname, national number, date of birth, gender, marital status, profile type, profile picture, sample signature, education degree, specialization, email address, mobile phone number, landline number, address, city, province, Postal code, bank account number

narration

In March 2019, a database containing the information of about 130 thousand users of the Ministry of Interior’s “Non-Governmental Organization Establishment System” was put up for sale in one of the hacker forums. The data included name, surname, national code, date of birth, gender, marital status, educational qualification, specialization, email address, address, postal code and other information of the users of this system. Unfortunately, there has been no reaction from the Ministry of Home Affairs or relevant news agencies regarding this information leak. The data was provided to Leakfa by a source who asked to be identified as “Dominic Vaughan”.

Leak date: March 8, 2019
Affected accounts: 126,170face viewThe magnitude of the leak116,000confirmedgeneral

Disclosed items

Full name, username, password, email address

narration

In December 2013, the largest social network in Persian language, “Face Nama”, was hacked by a person who calls himself “Mr_TOROJAN”. Minutes later, the extracted data, which included 116,000 unique email addresses along with names, usernames, and passwords with the MD5 algorithm, was posted on the site.

Leak date: January 10, 2013
Affected accounts: 116,478
In the news: Asr Iran reportKarbankThe magnitude of the leak106,000confirmedimportant

Disclosed items

Name, surname, date of birth, username, password, gender, landline phone number, mobile phone number, email address, profile picture, identifier, registration date, last entry date, work history, marital status, province, city, Address, degree, university, GPA, skills, resume, scanned documents

narration

In April 2019, a database containing the information of more than 100,000 users of the recruitment, job search, resume search and job advertisement service “Carbank” was put up for sale in one of the hacker forums. The information includes name, surname, date of birth, gender, username, password, landline phone, mobile phone, email address, work experience, marital status, city, province, address, degree, field of study and other information of users. It was the employees of this service. The data was provided to Leakfa by a source who asked to be identified as “Hermann Goering”.

Leak date: April 30, 2016
Affected accounts: 106,667my electricityThe magnitude of the leak79,000confirmedgeneralsample

Disclosed items

First name, last name, national number, mobile phone number, user ID, region code, city code, payment amount, payment date, tracking number, PSP company code, card number (incomplete), model ID, model name, make ID, warehouse Delivery and name of the electricity meter manufacturer

narration

In Mehr 1401, Barqman, the official portal for inquiry and payment of electricity distribution companies of the country, suffered a data leak. This data, which included name, surname, national number, mobile phone and other information of thousands of users related to this system, was placed on an unprotected Elasticsearch. At the request of users and in cooperation with security researcher Bob Dyachenko, Likfa is currently hosting sample data for this leak, if you have the original data, please contact us.

Leak date: 8 Mehr 1401
Affected accounts: 79,581
In the news: Barqnews reportJudiciary – Sana systemThe magnitude of the leak50,000confirmedgeneralimportantsample

Disclosed items

First name, last name, father's name, religion, gender, marital status, landline phone number, mobile phone number, phone number, national number, address, postal code, place of birth, place of residence, level of education, one-time password, password Personal, last password change date

narration

In February 2019, Sana's authentication system suffered a data breach. This data, which was put up for sale in one of the hacker forums, according to the seller, contains 25 million and 300 thousand lines of email address, date of birth, birth certificate number, name, surname, father's name, gender, landline phone, mobile phone, National code, address/address, place of birth, education level, one-time password (hashed), personal password (hashed) and other information of the users, the judiciary did not react to this incident at first, but a few days later, Mr. Mohammad Kazemi Fard, Deputy of Judicial Intelligence and Systems Affairs of the Statistics and Information Technology Center of the Judiciary, regarding the leakage of information of the users of the judicial electronic notification system, announced that there was no hacking or information leakage in the judicial system. At the request of users, Likfa is currently hosting sample data for this leak, if you have the original data, please contact us.

Leak date: 29 February 2019
Affected accounts: 50,432
In the news: Zomit report
Videos: Sana system information leak investigationAsiatechThe magnitude of the leak49,000confirmedgeneralsample

Disclosed items

Name, surname, national number, landline number, mobile number, ADSL number

narration

In June 2019, Asiatech, one of the Internet Service Providers (ISP) in Iran, suffered a data leak. This data, which was put up for sale in one of the hacker forums, contained the name, surname, national code, landline phone number, mobile phone number and other information of the company's employees and users. Asiatec first published the news in its official statement. Regarding the leak of users' information, he denied it, but the next day, according to a statement published in one of the media, they confirmed the data leak and announced that "the stolen information is related to one of the representative offices of this company." At the request of users, Likfa is currently hosting sample data for this leak, if you have the original data, please contact us.

Leak date: June 3, 2019
Affected accounts: 49,828
In the news: Zomit reportSharif University of TechnologyThe magnitude of the leak48,000confirmedimportant

Disclosed items

Name, surname, father's name, birth certificate number, national number, student number, gender, place of birth, date of birth, place of residence, life status, previous name and surname, landline phone number, mobile phone number, phone number, email address , username, password, job position, work history, address, city, province, zip code

narration

In December 2019, one of the servers of Sharif University of Technology, one of the most well-known universities in the country, was hacked by an unknown person. A few months later, a set of several databases containing name, surname, father's name, ID number, national code, gender, date of birth, email address, landline phone, mobile phone and other information of employees/professors and students of this university, It was put up for sale in one of the hacker forums.

Date of leak: 29 December 2019
Affected accounts: 48,492Khwaja Nasir UniversityThe magnitude of the leak45,000confirmedgeneralimportant

Disclosed items

Name, surname, father's name, national number, birth certificate number, place of issue, date of birth, gender, semester of entry, student number, field of study, course, course, grade point average, unit passed, conditional number, type of admission to the university, type of

quota , military status, religion, religion, marital status, mobile phone number, landline number, email address, place of birth, province of residence, city of residence, address or address, postal code, years of studentship

narration

In Shahrivar 1400, one of the systems of Khwaja Nasiruddin Tusi University of Technology, one of the top universities in the country, was hacked by an unknown person. A few days later, a collection of several databases containing about 100,000 lines of data was put up for sale on a hacker forum. These data included name, surname, father's name, national number, birth certificate number, place of issue and other identity and personal information of the students. The Research and Technology Vice-Chancellor of the University published a notice in this regard, which attributed the leaked information through the thieves' access to the personal files of the current affairs report of various university units.

Date of leak: 7 Shahrivar 1400
Affected accounts: 45,454
Official statement: University Research and Technology Vice-ChancellorEducational media for better gradesThe magnitude of the leak41,000confirmed

Disclosed items

Full name, username, user ID, password, city, email address, mobile phone number, device brand, device model, IMEI ID, Wi-Fi McAddress, software code version, software serial, Android version, Android ID, registration date, Internet connection status

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident finally led to the disclosure of about 42 thousand lines of name, username, password, city, email address, mobile phone number, mobile phone brand, mobile phone model, IMEI ID, Wi-Fi McAddress and other information of the users of the "Better Score Educational Media" software. " and several other services/software became "mobile pioneer company".

Leak date: January 24, 2019
Affected accounts: 41,890Etude Plus educational systemThe magnitude of the leak34,000confirmedimportant

Disclosed items

Name, surname, father’s name, national number, username, password, account type, mobile phone number, profile picture, contact list, father’s mobile phone number, mother’s mobile phone number, school ID, school name, school address, school principal’s name school principal’s cell phone, school principal’s username, school principal’s password, list of school classes, list of school entertainment bells

narration

In May 1400, a database containing the information of more than 34,000 users of the Etude Plus online training system was placed in one of the hacker forums. The data included name, surname, father’s name, national code, username, password, account type, mobile phone number, profile picture, contact list of father’s mobile phone number, mother’s mobile phone number and other information of users. This data included the first name, last name, father’s name, national code and mobile phone number of the teachers, as well as the contact list of the users of this system, which included about 200 thousand lines of first name, last name and mobile phone number, was also disclosed in this incident. Available for victim inquiries.

Leak date: May 26, 1400
Affected accounts: 34,071ClassinoThe magnitude of the leak30,000confirmed

Disclosed items

Name, surname, national number, educational level, field of study, province, gender, mobile phone number, user ID, registration date, account credit

narration

On December 1400, Classino, the first and largest online exam school and class in the country, experienced a data failure. This data, which contained more than 30 thousand lines of name, surname, national number, educational level, field of study, province, gender, mobile phone number and other information of users, was first put up for sale in one of the hacker forums. And then it was published publicly.

Date of leak: 8 December 1400
Affected accounts: 30,744Iranian language referenceThe magnitude of the leak24,000confirmed

Disclosed items

Username, password, IP address, email address

narration

In September 2016, the website of the country's most comprehensive language school on the web platform known as "Iranian Language Reference" was hacked by a group of hackers known as "Priv8_Team". This incident led to the disclosure of the site's database, which contained 24,000 lines of usernames, email addresses, passwords with the MD5 algorithm, and users' IP addresses.

Leak date: 11 Mehr 1396
Affected accounts: 24,898DeltafoxThe magnitude of the leak23,000confirmed

Disclosed items

Username, password, email address, website address

narration

In March of 2013, Deltafox, the download authority for computer games, was hacked by a person who calls himself "MR. HOSSEIN". This incident led to the disclosure of the site's database, which contained 23,000 lines of usernames, email addresses, passwords with the MD5 algorithm, and website addresses of users.

Leak date: April 3, 2014
Affected accounts: 23,214Payam Noor UniversityThe magnitude of the leak19,000confirmedimportant

Disclosed items

Name, surname, student number, father's name, date of birth, birth certificate number, serial number of birth certificate, national number, military status, marital status, province, city, postal code, place of residence, place of birth, landline phone number, mobile phone number , email address, school name, grade point average, 3×4 photos

narration

In July 2019, the website of Payam Noor University, one of the top universities in the country, was hacked by an unknown person. A few months later, a database from this site containing more than 19 thousand lines of first and last name, father's name, date of birth, birth certificate number, national code, mobile phone number, email address and other personal information of students, in one of the hacker forums. It was put up for sale. In Mehr 1400, we witnessed a new data leak from this university, a collection containing more than 13 thousand lines containing identity information, student information, certificate date, certificate number, and landline and cell phone numbers of students. The possibility of querying this data is also available for the victims.

Leak date: July 24, 2019
Affected accounts: 19,155Tehran University of Medical SciencesThe magnitude of the

leak18,000confirmed

Disclosed items

First name, last name, national number, email address, username, password, landline phone number, mobile phone number, emergency contact number, father’s cell phone number, mother’s cell phone number, IP address, user ID

narration

On March 3, 2019, a database containing the information of more than 18 thousand students of “Tehran University of Medical Sciences and Health Services” which included name, surname, national code, email address, username, password, mobile phone number and other information. , was put up for sale in one of the hacker forums. One of the other systems of this university suffered a data leak last month, which eventually led to the disclosure of the information of 3,000 of its employees, including name, surname, father’s name, national code, ID number, job position, landline number, Cell phone numbers, latest salaries and other information are available for victim inquiries.

Leak date: March 3, 2019
Affected accounts: 18,507Luxa PlusThe magnitude of the leak14,000confirmed

Disclosed items

Name, surname, mobile phone number, email address

narration

In November 2016, Luxa Plus, a social network designed to provide VIP services to the affluent segment of the society, was hacked by an unknown person. 3 years later, its database containing more than 14,000 user information, including first and last names, email addresses and mobile phone numbers, was put up for sale on a hacker forum.

Leak date: November 30, 2016
Affected accounts: 14,725IranplastThe magnitude of the leak14,000confirmed

Disclosed items

Full name, landline phone number, mobile phone number, password, email address, place of residence, company name, company website address, company activity, company registration number

narration

In December 2018, the website of the international exhibition of plastics, rubber, machinery and equipment known as “Iranplast” was infiltrated by a group of hackers known as “Liosion Team”. This incident led to the disclosure of the information of about 17 thousand traders from all over the world (14 thousand from Iran) who had registered to receive services in this exhibition.

Date of leak: December 30, 2018
Affected accounts: 14,716Samsung CenterThe magnitude of the leak12,000confirmed

Disclosed items

First name, last name, landline phone number, mobile phone number, password, IP address, email address

narration

In April 2013, the website of the official sales representative of Samsung products since 2007 in Iran, known as “Samsung Center”, was hacked by a group of hackers known as “Zurael sTz”. This incident led to the disclosure of about 20,000 data containing 12,000 personal information of customers, including names, surnames, email addresses, mobile and landline numbers, IP addresses and passwords with the MD5 algorithm.

Leak date: April 18, 2016
Affected accounts: 12,992Parsman Islamic softwareThe magnitude of the leak9,000confirmed

Disclosed items

User ID, email address, mobile phone number, device brand, device model, registration date

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident finally led to the disclosure of about 9 thousand lines of user ID, email address, mobile phone number, mobile phone brand, mobile phone model and other information of users of “Persman Islamic Software” and several other services/software of “Pishgaman Moj Mobile Company”.

Leak date: January 24, 2019
Affected accounts: 9,099Ports and Maritime OrganizationThe magnitude of the leak9,000confirmedgeneralimportant

Disclosed items

Name, surname, father's name, national number, birth certificate number, serial number of birth certificate, date of birth, religion, gender, marital status, date of marriage, spouse's occupation, number of children, organizational position code, signatory's name, signatory's job position, last salary date of official employment (permanent), date of contract employment (temporary), military status, duration of military service, mobilization status, address, postal code, landline phone number, mobile phone number, email address, place of birth

narration

In October 2019, the Iranian Ports and Maritime Organization witnessed a massive cyber attack against its infrastructure, about 48 hours later, a large collection of about 15 gigabytes of data of this organization, including the information of employees, customers, contracts, shipments, payments and information Another of various ports such as Bandar Bushehr, Imam Khomeini, Shahid Rajaei and Shahid Bahnar was included in a telegram channel. The Ports and Maritime Organization of Iran, while confirming that the infrastructure of this organization has been targeted by a cyber attack, announced that preventive and appropriate measures have been taken against this attack and the missions of the Ports and Maritime Organization are ongoing without interruption. In an announcement, the Maher center announced the cyber attack on two government organizations, although it did not name them, and announced the temporary suspension of some services and technical tests of these centers as a precaution after receiving the warnings.

Date of leak: 22 Mehr 1399
Affected accounts: 9,749
In the news: Moj reportIran's security teamThe magnitude of the leak6,000confirmed

Disclosed items

Username, password, IP address, email address, date of birth

narration

In July 2013, Iran's security team, a specialized authority on hacking and security, was infiltrated by a group of hackers known as "ISG & RST". A few months later, its database was posted on a popular hacker forum, containing more than 6,000 usernames, dates of birth, email addresses, IP addresses, and MD5 passwords.

Leak date: July 7, 2013
Affected accounts: 6,523Shia daily calendarThe magnitude of the leak6,000confirmed

Disclosed items

User ID, email address, mobile phone number, device brand, device model, registration date

narration

In Mehr 2019, the hosting server of Azan Go Badsaba calendar, one of the most installed and popular Iranian software, was hacked by an unknown person. Aggregating the main and supporting data of different software on one server and not following the basic principles of security and network security made it easy for an intruder to take control of other software by infiltrating the server of one software. This incident finally led to the disclosure of about 7 thousand lines of user ID, email address, mobile phone number, mobile phone brand, mobile phone model and other information of the users of “Shi’a Zahi Calendar” and several other services/software “Pishgaman Moj Mobile Company”. became.

Leak date: January 24, 2019
Affected accounts: 6,758Check light forumThe magnitude of the leak5,000confirmed

Disclosed items

User ID, Username, Email Address, IP Address, Password, Salt

narration

In Mehr 2019, Chirag Chek Association, a specialized authority on the basics of electrical and automotive electronics, suffered a data leak. A few months later, a database containing the information of more than 6,000 users of this website, including user IDs, usernames, passwords, salt, email addresses, and IP addresses of users, was released among hacking forums and groups.

Date of leak: 10 October 2019
Affected accounts: 5,970Post office – Sarpol ZahabThe magnitude of the leak5,000confirmed

Disclosed items

First name, last name, father’s name, national ID number, birth certificate number, date of birth, tracking code, sending date, landline phone number, mobile phone number

narration

In April 1400, a database containing the information of more than 5,000 customers of the Islamic Republic of Iran Post Company was put up for sale in one of the hacker forums. Name, surname, father’s name, national number, birth certificate number, date of birth, tracking code, date of sending, landline phone number and mobile phone number. The data was provided to Leakfa by a source who asked to be referred to as “DeathAngle”.

Leak date: April 5, 1400
Affected accounts: 5,394

Iranian information leak tracking system