



Deloitte Cyber & Technology News digest

Issue #15

Azerbaijan

Kaspersky calls on Azerbaijani social network users to be vigilant

Recently, the Interior Ministry warned citizens about fraud on social networks. According to the ministry, in recent years, some fraudsters have obtained bank card information claiming that they are far away or not in the country, in order to buy products sold by citizens who trade on social media and advertising sites.

Source: xeberler.az, July 1, 2021

Issuance of electronic health cards may be suspended in Azerbaijan

The issuance of electronic health cards will be stopped in Azerbaijan in the near future. The statement came from the Health Informatization Center of the Ministry of Health. The center noted that health and other information about citizens will be integrated into their ID cards. Source:

xeberler.az, July 1, 2021

Azerbaijan ranks in the top 3 in the CIS for cyber security

Azerbaijan has improved its position among the world's countries in terms of cyber security by 15 points over the past two years, and is now in third place in the CIS region, rising by one point. This is stated in the annual release of The Global Cybersecurity Index (GCI) for 2020, published by the International Telecommunication Union (ITU). According to the report, Azerbaijan scored 89.31 out of a possible 100 points, which was calculated in 5 categories. Thus, official Baku scored 20 points on legal measurements, 19.19 points on technical measurements, 13.14 points on organizational measurements, 16.99 points on capacity development and 20 points on cooperative measurements.

Source: xeberler.az, July 5, 2021

Azerbaijan will sign a regional roaming agreement with the "Eastern Partnership" countries

Azerbaijan will sign a regional roaming agreement with the countries joining the Eastern Partnership initiative. The statement came from the Azerbaijani Ministry of Transport, Communications and High Technologies. It was noted that the ministry has been cooperating closely with telecommunications regulators of both the Eastern Partnership countries and the European Union (EU) for many years. According to the agreement to be signed with the Eastern Partnership countries, our citizens will be able to benefit from favorable roaming tariffs when traveling to Georgia, Ukraine, Belarus and Moldova in the future.

Source: xeberler.az, July 9, 2021

Methods of e-learning management are being developed in Azerbaijan

In Azerbaijan, the Education 4.0 platform is developing methods to increase the efficiency of e-learning management through the application of Data Mining technology. The statement came from the Institute of Information Technology of the Azerbaijan National Academy of Sciences. The introduction of technologies such as Data Mining and Big Data on the Education 4.0 platform is a matter of time, the institute said.

Source: xeberler.az, July 13, 2021

A national anti-plagiarism service is being established in Azerbaijan

The Institute of Information Technologies of ANAS is developing the concept of creating a national anti-plagiarism service. According to the institute, the concepts of plagiarism and piracy, types of plagiarism and its causes were identified within the work done. Methods of combating plagiarism including anti-plagiarism software were analyzed according to key indicators. Anti-plagiarism services have been investigated in Azerbaijan, and the Anti-Plagiarism Service has been launched at the Institute.

Source: xeberler.az, July 15, 2021

A Cyber Attacks Simulation Laboratory has been established at the ICC

A Cyber Attacks Simulation Laboratory has been established under the Information Computing Center of the Ministry of Transport, Communications and High Technologies. The laboratory will study cyber security processes, train specialists in this field, and carry out counteractions against

possible cyber attacks. It is also planned to check the gaps in the systems and provide security audit services. In the laboratory, where experts will conduct regular simulation attacks, it will be possible to prepare projects of the institution, as well as IT reports for use by other entities.

Source: xeberler.az, July 16, 2021

SOCAR and its partners organize professional cyber security courses

The State Oil Company of Azerbaijan (SOCAR) organizes professional courses on cyber security and data analysis from July 2021 to February 2022 in order to successfully implement one of the strategic goals of digital transformation and develop local human resources in this field. The main purpose of the courses organized within the framework of SOCAR Midstream Social Investment initiatives is to fulfill the tasks arising from the Decree of the President of the Republic of Azerbaijan dated April 27, 2021 on "Improving governance in the field of digital transformation", increase knowledge and skills of individuals interested in data analysis and cybersecurity, create interest and motivation among young people in these areas helping to boost their career potential.

Source: xeberler.az, July 28, 2021

CIS

Russia

The share of intentional leaks of confidential data in Russia has exceeded the global number

"Kommersant", referring to InfoWatch reports that the share of intentional leaks of confidential data in Russia in 2020 exceeded the world figures and reached 79.7%. In general, the Russian Federation accounted for 16.9% of the global volume of information leaks. More than 40% of them were in technology and finance. In just a year, more than 100 million personal data and payment information records have leaked. The number of deliberate leaks from commercial and government organizations in Russia increased by 60% over the past year.

Source: banki.ru, July 5, 2021

Banks record growth of cyberattacks on their systems

Russian banks record an increase in attempts by cybercriminals to attack their information infrastructure: every week SberBank sees about 100 cyber attacks on information systems and services, the number of DDoS attacks quadrupled in January-April compared to last year; at VTB - 1.2 million attempts in five months of this year, while for the entire last year there were 750 thousand; Credit Bank of Moscow also notes an increase in the number of attacks and associates this with the shift of crime to the cyberspace, writes "Vedomosti" citing representatives of credit institutions.

Source: banki.ru, July 6, 2021

Experts have warned of the top cyber threats of 2021

The most common type of fraud in 2021 is direct attacks on bank customers using social engineering, according to a report from YuMoney. The company's experts noted that they are

talking about hundreds of millions of unauthorized transfers according to reports from the Central Bank. Also, one of the cyber threats is ransomware trojans - ransomware attacks on organizations through known vulnerabilities.

Source: banki.ru, July 9, 2021

Sberbank admitted the likelihood of hacker attacks on large companies in Russia

SberBank admits the likelihood of hacker attacks on large companies in Russia, as was the case in the United States, when cybercriminals paralyzed the activities of the largest enterprises, causing great damage to them. Stanislav Kuznetsov, deputy chairman of the board of Sberbank, told reporters on the couloir of Cyber Polygon, TASS reports. Kuznetsov noted that today the most dangerous threats are virus infections and virus ransomware, which are now being actively spread by hackers.

Source: banki.ru, July 9, 2021

Media: Central Bank warned of attacks on banks through participants in their ecosystems

The Central Bank informed about the risks of "infection" of banks through participants in their ecosystems, mainly small organizations that have access to information resources of parent organizations, their databases. At the same time, ecosystem participants in many cases are not able to independently assess risks and ensure information security; if attackers are interested in attacking ecosystems, they simply find a weak link, "Vedomosti" writes, referring to a representative of the Central Bank.

Source: banki.ru, July 14, 2021

Experts talked about cyber risks for companies posed by remote employees

The transition to a remote mode of operation significantly increases cyber risks for companies, "Izvestia" writes. This is stated in a study by Check Point. The most significant increase in the number of attacks was reported by representatives of the financial (54%), utilities (52%) and manufacturing (47%) sectors. Many companies use several disparate solutions, it is more difficult for IT specialists and security experts to manage them, they do not see the entire threat landscape, said Alexey Beloglazov, head of the group of systems engineers working with partners at Check Point Software Technologies.

Source: banki.ru, July 15, 2021

Fraudsters began to fake bank websites more often in 2021

In 2021, fraudsters began to fake the websites of Russian credit organizations more often: at the moment, 3,258 pseudo banks have already been identified, which is 75% of the number discovered last year, RIA Novosti told Bi.Zone. It is noted that phishing sites copy banks' web resources as closely as possible: scammers adjust the interface to various credit institutions and redraw the design of well-known banking products.

Source: banki.ru, July 26, 2021

Experts notified about the emergence of a service that can help hackers in writing a code

The Copilot service, created on the basis of a neural network and designed to simplify the work of programmers, can be used by malware developers, "Izvestia" writes. This is the conclusion reached by Russian cybersecurity experts.

Source: banki.ru, July 28, 2021

Testing of Face Pay technology with the participation of passengers began in the Moscow metro

Testing of Face Pay technology with the participation of passengers begins in the Moscow metro, according to the press service of the Moscow Department of Transport and Road Infrastructure Development. At the first stage, testing of the service will involve 1,000 passengers. Those interested can take part, for this one needs to fill out an application. It is noted that the Moscow metro is the leader in terms of the number of fare payment methods, and all of them will remain. Face Pay will be another convenient service for passengers, but not mandatory. "We are sure that this method will be chosen by tens of thousands of Muscovites who follow trends and love modern technologies," the press service emphasized.

Source: banki.ru, July 31, 2021

Kazakhstan

The amount of cyberattacks in the Republic of Kazakhstan has grown by 20% per year

According to the KZ-CERT computer incident response service, over 13.9 thousand information security incidents were registered in the first half of this year, which is 20.1% more than in the same period last year. This is the highest rate ever recorded.

Source: profit.kz, July 8, 2021

Kazakhstan ranks 9th in the world in terms of risk of infection on the Internet

In a recent report by the UN International Telecommunication Union, it was reported that Kazakhstan was ranked 31st in the world cyber readiness rating. According to experts, the strengths of Kazakhstan's cyber readiness are technical, legislative and cooperative measures aimed at creating and strengthening technical institutions and partnerships between bodies involved in ensuring information and cyber security. As for cyber threats, Kazakhstan confidently ranks among the top lines of the ratings for various indicators.

Source: profit.kz, July 8, 2021

Kyrgyzstan

Kyrgyzstan climbs 19 positions in cybersecurity indicators

According to the global cybersecurity index, Kyrgyzstan rose from 111th position to 92nd in the period from 2018 to 2020. Such data are provided by the Ministry of Digital Development. Kyrgyzstan also showed growth in the field of cybersecurity being in seventh place among the CIS countries, by the end of 2020. The Global Cybersecurity Index takes into account legal, technical, and organizational indicators.

Source: 24.kg, July 2, 2021



deloitte.az

Deloitte adı Deloitte Touche Tohmatsu Limited şəbəkəsinə daxil olan üzv şirkətlərdən birinə və ya bir neçəsinə və əlaqədar müəssisələrinə aid ola bilər. DTTL ("Deloitte Qlobal") və bu şəbəkəyə daxil olan hər bir üzv şirkət ayrı-ayrılıqda hüquqi şəxslər və müstəqil müəssisələrdir. DTTL müştərilərə xidmətlər göstərmir. Ətraflı məlumat üçün www.deloitte.com/about səhifəsinə daxil olun.

Deloitte qlobal səviyyədə audit və əminlik, konsaltinq, maliyyə, risk, vergi üzrə məsləhət xidməti və digər əlaqədar xidmətlər göstərən aparıcı markalardandır. 150-dən çox ölkədə və ərazidə xidmətlər göstərən üzv şirkətlər şəbəkəsi Fortune Global 500® üzrə beş şirkətdən dördünə öz xidmətlərini göstərir. Deloitte-un təxminən 330,000 peşəkar mütəxəssisinin təklif etdiyi fərq yaradan həllər haqqında ətraflı məlumat üçün www.deloitte.com/about səhifəsinə daxil olun.

Bu məlumatda yalnız ümumi informasiya əks olunur və Deloitte Touche Tohmatsu Limited şirkətlərindən, onun üzv şirkətlərindən və ya əlaqədar müəssisələrdən (birlikdə "Deloitte Şəbəkəsi") hər hansı biri bu məlumat vasitəsilə peşəkar məsləhətləşmə və ya xidmətlər təmin etmir. Maliyyə fəaliyyətinizə və ya müəssisənizə təsir göstərə biləcək hər hansı qərarlar qəbul etməzdən və ya tədbirlər görməzdən əvvəl peşəkar mütəxəssis ilə məsləhətləşmək daha məqsədəuyğundur. Deloitte Şəbəkəsinə daxil olan heç bir müəssisə bu məlumata istinad edən hər hansı şəxsin məruz qaldığı zərərə görə məsuliyyət daşımır.

Nobel pr. 25E, Bakı Ağ Şəhər Ofis Binası
Bakı, AZ1025, Azərbaycan Respublikası

© 2021 Deloitte & Touche MMAC. Bütün hüquqlar qorunur.