Deloitte.

Cyber security review of banks in Azerbaijan

November 2022

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Organizations around the world continue to face security breaches, even those that have made significant investment in security technology. On the one hand, this has been caused by bad actors quick to evolve in cyber attack tactics and stay ahead of the technology curve. On the other, the enterprise cyber risk landscape has change significantly due to number of factors, such as:

1. More remote workers. After COVID pandemic more and more people prefer to work from home.
2. Increased network-connected devices. When seeking a soft attack vector, cybercriminals are able to choose from a growing number of network-connected physical assets, of which should be 29.3 billion by 2023, according to estimates.*
3. A broader ecosystem of third-party partners, as more and more banks integrate outsourcing and cloud providers into their services and business processes.

Meanwhile, the cost of cybercrime continues to climb; from US$3 trillion in 2015 to potentially US$10.5 trillion by 2025.**

The cybersecurity agenda in Azerbaijan banks is growing in tandem with the rest of the world. Even though the banks are trying to solve the problem in their own way, the vast majority of them are actually protecting their critical assets against the same threat landscape.

As such, the objective of the study is to understand the ability of Azerbaijan banks to identify and address basic cybersecurity risks and their trends in time.

This year, we expanded the scope of the study to include, in addition to banks operating in Azerbaijan, their peers in Kazakhstan and Uzbekistan, allows us to compare general bank cyber maturity in the region.

Although most of the research areas have remained unchanged, we still made minor changes to extend the list of areas for analysis.

It is also worth noting that we included the corresponding portals for corporate and retail clients in the scope of analysis in addition to the public Internet bank servers. In total, we analyzed a total of 44 web resources in Azerbaijan.

We sincerely hope that you find the report informative and useful. Please contact us if you have any questions or suggestions regarding the information provided in it.

Vladimir Remyga
Director
Cyber Risk Advisory

*- Cisco, *Cisco annual internet report (2018–2023) white paper* , accessed November 17, 2021.
**- Steve Morgan, "*Cybercrime to cost the world $10.5 trillion annually by 2025* ," Cybersecurity Ventures, November 13, 2020

Deloitte Azerbaijan has conducted its third annual cybersecurity study of banks in Azerbaijan.

44 publicly available internet resources were analyzed.

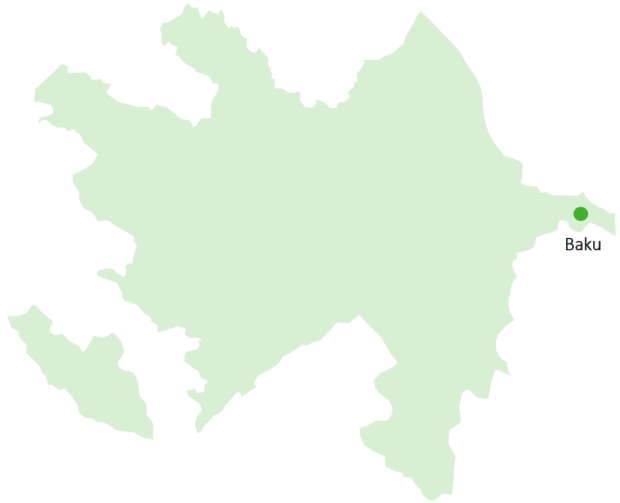
Deloitte in Azerbaijan

Deloitte & Touche LLC is the DTTL member firm in Azerbaijan. Deloitte has been operating from its Baku office since 2002.

Deloitte is a recognized leader in the information security consulting market. The firm has been praised by industry analysts including Gartner, Forrester, and Kennedy.

Since it began operating in Azerbaijan, Deloitte has implemented hundreds of successful projects for financial institutions, government organizations, and industrial and commercial enterprises, supporting the largest transnational projects and being a leader in providing services to the banking sector. To date, the company is represented by a main office in Baku, which employs more than 200 local and foreign audit, consulting, financial advisory, and tax & legal experts.

Our experts have developed fully tailored solutions for companies to meet the growing demand for cyber security services. Our products include advanced cyber security incident detection and monitoring solutions, threat intelligence analysis, cyber threat management, incident response, and others.



Deloitte Cyber Offering

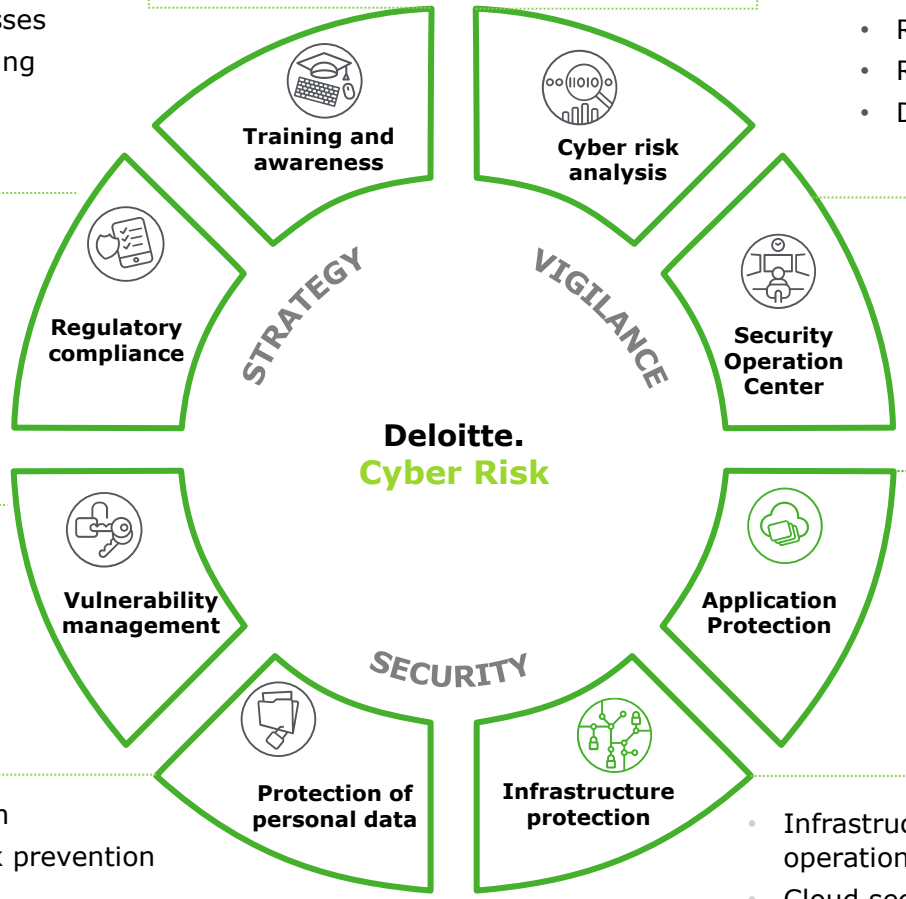
As a worldwide leader in cyber strategy consulting and cyber intelligence, Deloitte in Azerbaijan offers a fully customizable suite of cyber solutions and managed services. With a commitment to technological innovation and broad industry expertise, our Deloitte global network gives us the insight and experience to face any local scenario.

- Implementation of information security awareness processes
- Information security training

- Risk identification
- Risk modeling and assessment
- Data analysis

- Implementing a cyber risk management process
- Compliance assessment and preparation for certification: ISO 27001, PCI DSS, SOX 404
- Digital risk management

- Outsourcing Security Operation Center (SOC) services
- SOC analytics L1 & L2 & L3
- Malware analysis



- Developing and executing vulnerability management processes
- Vulnerability management tool system integration

- Security testing of applications and systems
- Source code security analysis
- Analysis of development security

- Personal data protection
- Implementing data leak prevention programs

- Infrastructure penetration testing, including operational technology (SCADA)
- Cloud security assessment
- PKI design
- Security setting improvements

Our approach: Methodology

In order to understand the banks' ability to identify and address cybersecurity risks, we assessed their public internet resources and mobile applications for well-known and widespread cyber threats and vulnerabilities. For this, we developed and automated a methodology that was capable of covering a wide range of cyber matters, including security, availability, confidentiality, integrity and privacy. The methodology applies a set of open frameworks, such as open-source intelligence (OSINT) and Open Web Application Security Project (OWASP).

The methodology consists of the following 4 stages:

Stage 1: Subject redefinition

In previous years, the study covered the following eight subject areas: Site Availability, Domain Reputation, HTTP security, Traffic protection, Leaked e-mail addresses, GDPR Compliance, Open Ports and Cybersquatting. This year, we added Mobile banking security and Mail server security. We also replaced Cybersquatting with Log4J Vulnerability.

Stage 2. Objects clarification

The intention was to compile a list of bank websites to be studied. However, since this Report is the third one we have compiled, we have had to update the list of active banks operating in Azerbaijan.

In previous years, we only analyzed the banks' main websites. However, the banks often dedicate separate websites to serve individuals and/or corporate clients alongside their main website. For this reason, we added new Corporate and Retail site subcategories for analysis this year.

Stage 3. Data gathering

For the analysis, we used a set of open online tools such as Google PageSpeed, SSLLabs, Talos Intelligence, Trusted Source, Haveibeenpwned and others. A detailed description of the tools used is given separately at the beginning of each of the sections or is given directly next to the description of the metrics and parameters being checked.

Stage 4. Analysis, comparison and reporting

During the final stage, we analyzed and verified all data collected. Analysis findings are provided in the Report and accompanied with comparative graphs showing current and previous year's results.

Our approach: Test categories

Site availability. Today, websites are one of the main tools for banks to interact with companies and individuals. For example, performance, which includes metrics such as response time, first render content, and first input latency plays a key role in website availability during DDOS attacks. The speed of response directly affects website usability - the user immediately receives the requested result without a long waiting time.

Domain reputation. Domain reputation is one of the key aspects of trust relationships in cyberspace. A less reliable measurement of domain reputation results in a lower ranking in search engine listings. This can lead to emails sent from the bank's domain being marked as spam.

HTTP Security. An effective method of protecting domain security is to set HTTP headers correctly. Since servers are always waiting for requests, it will not be difficult for attackers to use the server response to compromise a site or find security weaknesses, and exploit them further.

Traffic protection. In HTTPS, data is encrypted using a Transport Layer Security protocol, and earlier by Secure Sockets Layer. These cryptographic protocols are the most popular methods of ensuring secure communication over the Internet. Digital certificates authenticating the domain and site owner must be installed on a server to establish an SSL/TLS connection. This is required to ensure that the user is visiting a genuine resource, and not a fake page created by an attacker. This assessment category involves checking for earlier versions of security encryption protocols in use, i.e. checking for known vulnerabilities, mainly SSL-related, but also outdated versions of TLS (TLS 1.0, 1.1).

Mail server security. The main problem with using e-mail is a lack of security. Email weaknesses give attackers a free hand to launch attacks capable of compromising companies, whether through spam, malware, phishing attacks, sophisticated targeted attacks, or leaking corporate email addresses to the public.

Our approach: Test categories

Leaked email addresses. Organizations must be ready to deal with situations where corporate email registration results in the leakage of an employee's credentials on websites. Technically less-aware people may use the same or similar credential choices across multiple web applications, and leaked passwords and corporate email passwords may or may not differ slightly, which may result in the risk of a loss of finances, customer confidence, and reputation**.**

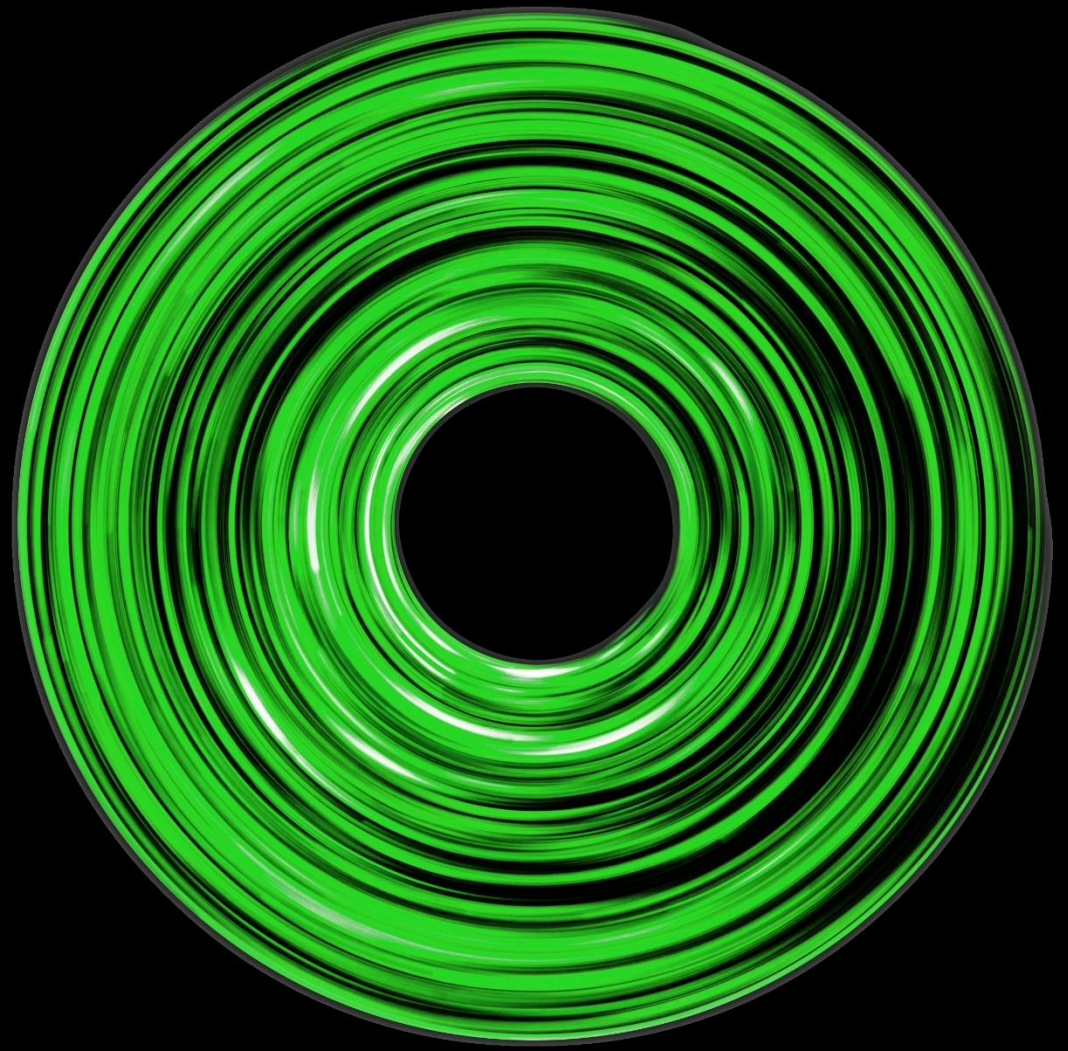
GDPR Compliance. The GDPR, or the General Data Protection Regulation, is an EU data protection and privacy regulation that applies to all persons in the European Union. According to paragraph 2 of article 3 of the GDPR, which deals with territorial coverage, it says that even companies established outside the EU are subject to the requirements of the GDPR if they offer goods or services to persons (data subjects) residing in the EU or monitor the behavior of such persons regardless of whether payment is required from the data subject. In other words, if any bank stores the data of at least one client from the EU, it is automatically subject to the GDPR.

Open ports. Improving the security of web servers by reducing attack vectors should be a key task for administrators. This can be achieved by installing and maintaining only the necessary services (ports) that allow access to internal and external clients.

Mobile banking security. The specificity and sufficient openness of mobile platforms make mobile device users a convenient target for intruders. A whole arsenal of hacking programs and tools exist for mobile platforms, such as viruses, trojans, fake banking programs, ransomware, and all kinds of spyware. Thus, checking the security of mobile applications is an essential assessment to protect user data and bank resources from potential threats.

Log4j Protection. Log4Shell vulnerability works by using a Log4j feature that allows users to specify their code to format a log message. For example, the function allows Log4j to log not only a username associated with each server login attempt but also a real username if a separate server maintains a directory linking usernames and real names. This, in turn, gives the attacker information regarding server and user data, with the aim of phishing attacks and compromising confidential data.

Summary of results



Executive Summary

This year's results have shown **multi-directional trends**. For example, despite the improvements demonstrated by Azerbaijan banks in some areas, other areas have registered negative changes, and as such, the **overall bank cyber security rating increase up 10% on the previous year** (refer to slide 10 for more details).

However, when it comes to comparing the results of Azerbaijan banks against their peers from Kazakhstan and Uzbekistan, then the **current situation is not so optimistic**. Kazakhstan leads with an overall rating of 72.3%, followed by Uzbekistan with 71.6% and Azerbaijan third with 64.6%. There is no area where banks in Azerbaijan are recognized as leaders (refer to slide 11 for more details).

Another interesting outcome of the study, and a real challenge for Azerbaijan banks, is **Mobile Banking Security**. Their score in this area is one of the lowest compared to other areas of the study. The increasing demand for mobile banking services coupled with insufficient attention to cyber matters should be treated as a negative factor that increases the risk of possible cyber security breaches through mobile devices.

Generally speaking, the results of the study indicate that a number of **banks in Azerbaijan still have a high cyber risk appetite**. They tend to identify cyber risks incorrectly and underestimate their consequences, failing to address the risks as intended. The situation is aggravated in the context of external geopolitical factors, when foreign countries or organized hacker groups frequently compromise the cyber security of critical infrastructure elements, such as banks.

How can banks adapt to this atmosphere of heightened risk?

First of all, Azerbaijan's need to enforce more **comprehensive and sustainable cyber rules** that target the current threat landscape. This could be accompanied by **cyber security risks and event-sharing** options for banks, which will lead the banks in Azerbaijan to improve cyber maturity and better respond to hacker attacks.

Secondly, existing regulations, which require that all banks implement **Information Security Management Systems** should be tailored, explained and implemented. Bank management must understand their purpose and approach, and use them not only as a compliance issue but also as an element of the leading information security standard - ISO 27001 whose purpose is to make cyber management matters transparent and related investment decisions reasonable to the business.

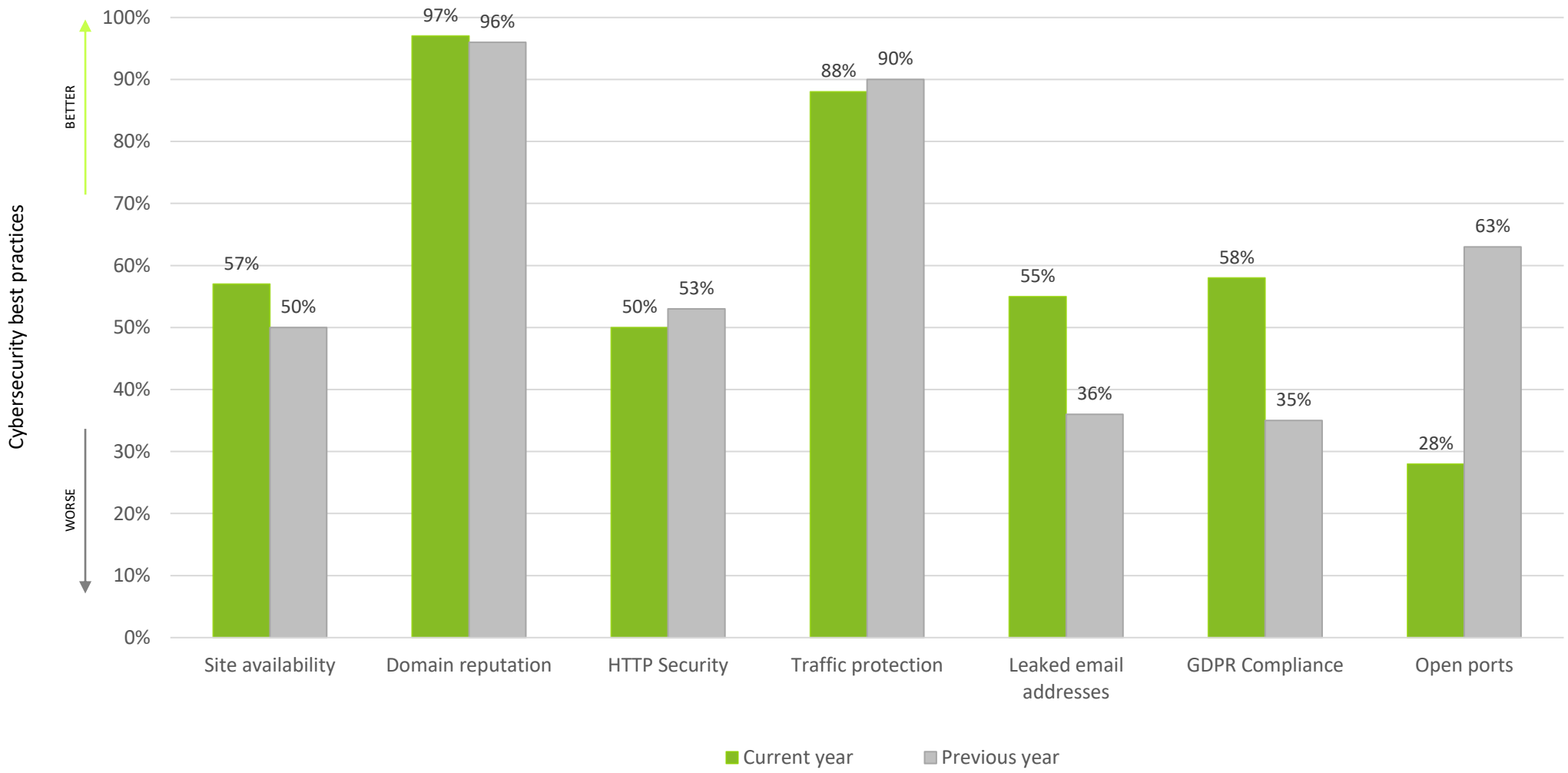
Thirdly, a **cyber risk treatment plan** must cover identified cyber risks appropriately and efficiently, and incorporate rise-up user and bank client awareness, up-to-date cyber security policies and procedures, securely configured IT infrastructure, digital forensic and incident response tool setup.

And finally, the second and third lines of defense should **actively monitor and regularly evaluate** existing security measure completeness and accuracy, applying all of the required corrective actions if needs be.

Bottom line

The goal of cybersecurity is to maintain safe and stable business operations even in the face of cyber risks. Each bank has to assess its risks individually. Some risks will be critical and others not. Nevertheless, almost all cyber attacks begin through simple vulnerabilities and the gathering of limited rights in target IT systems. Only then bad actors are trying to elevate the right to obtain privilege or administrative rights and compromise whole target infrastructure. For this reason, **there are no insignificant cyber risks**; they all need to be addressed properly and in good time.

Comparison of data from the current and previous year's reports
Results for Azerbaijan banks in the main website category



Benchmark indicators of the three countries for each Report section
Summary result for all three site categories

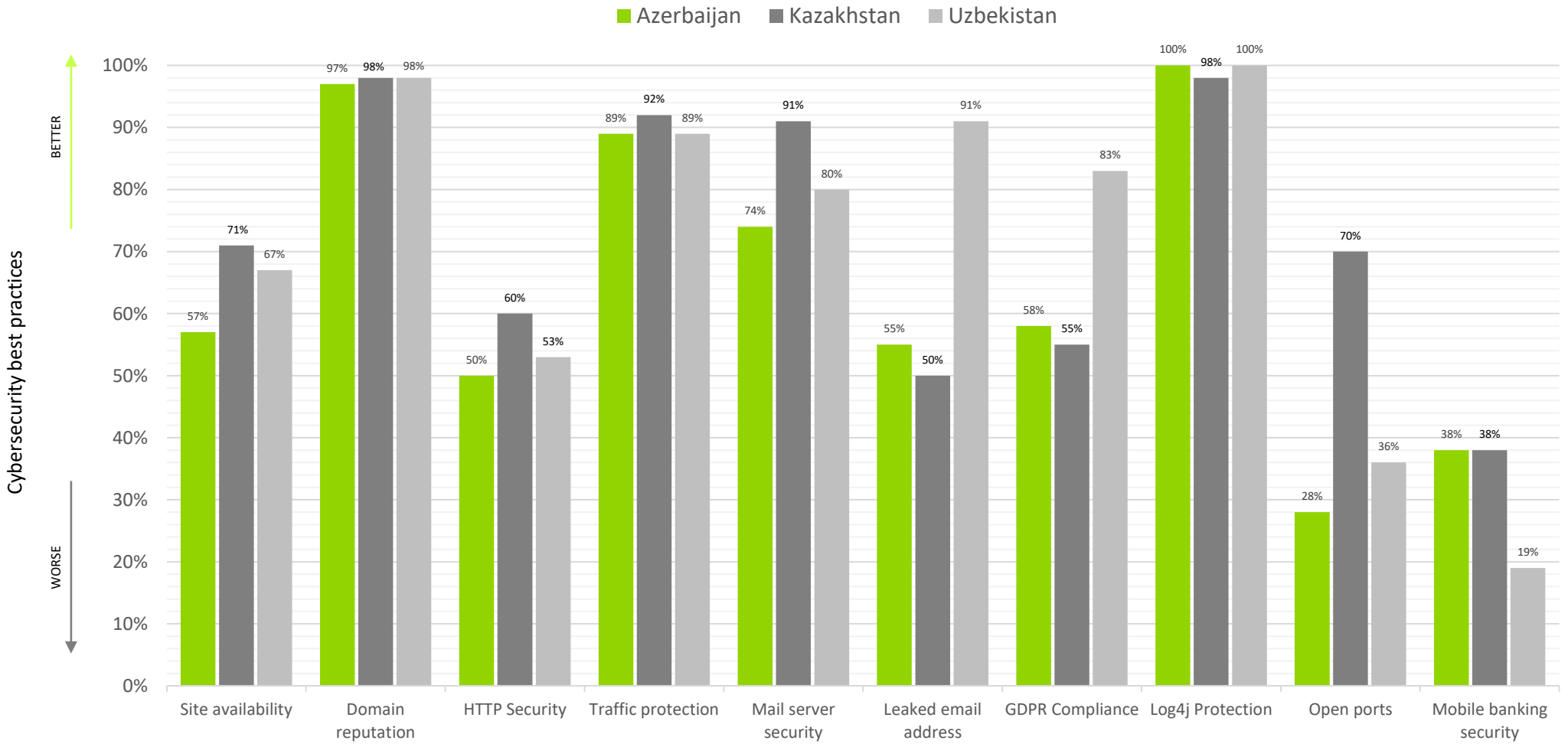
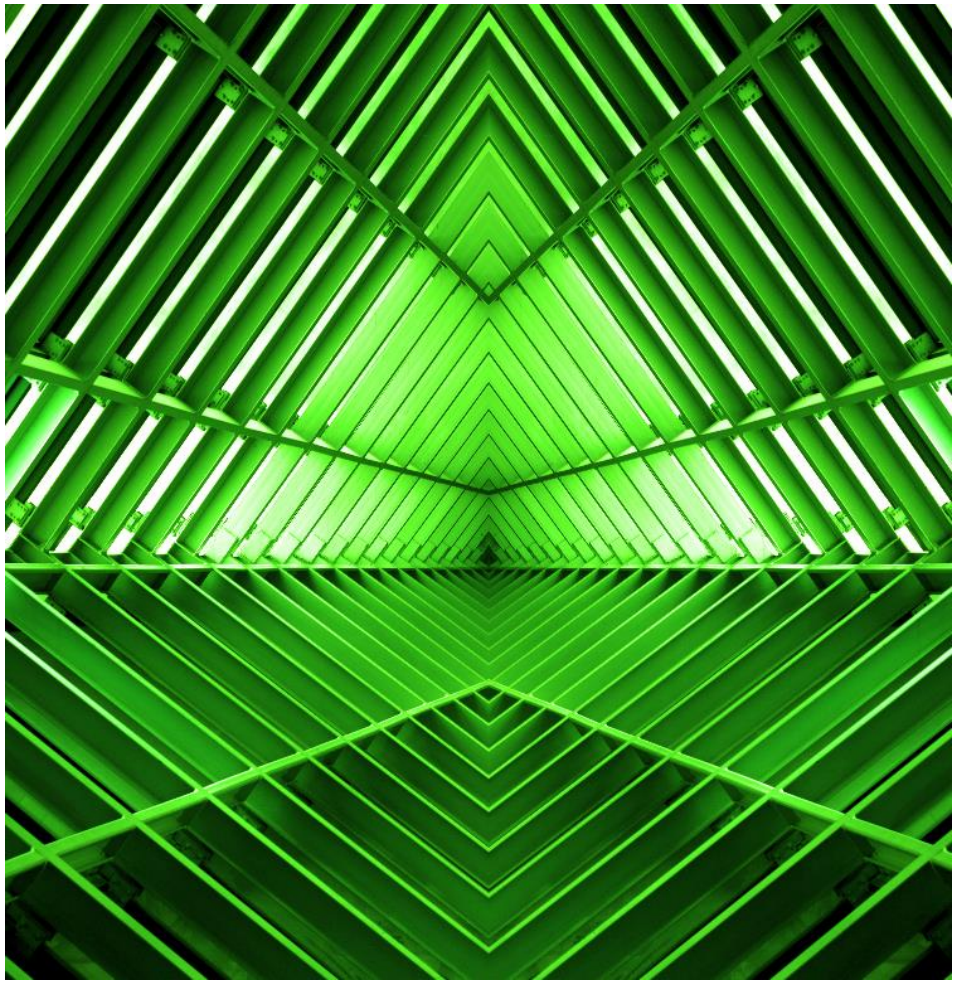
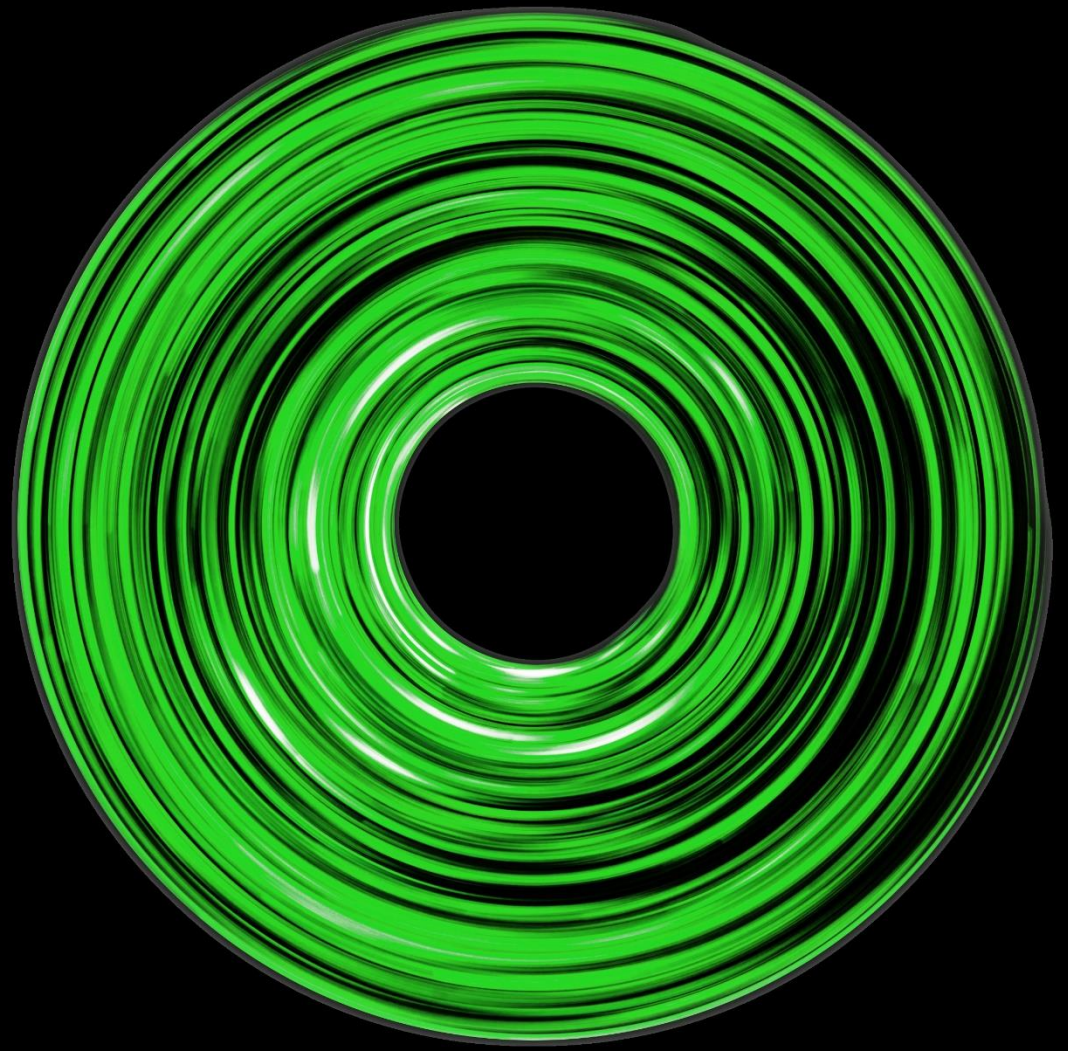


Table of contents



1. Site availability



1. Site availability

The architecture of server and network infrastructure; Internet portal configuration, and directly optimized Internet site content are the key factors in ensuring the customer availability of bank Internet resources. In particular, these factors are important in terms of protecting bank online resources from DOS attacks*.

Today, there are many ways to evaluate site performance. However, for the purposes of this study, we selected the following three metrics:

1. First Input Delay (FID);
2. Response Time (RT);
3. First Contentful Paint (FCP).

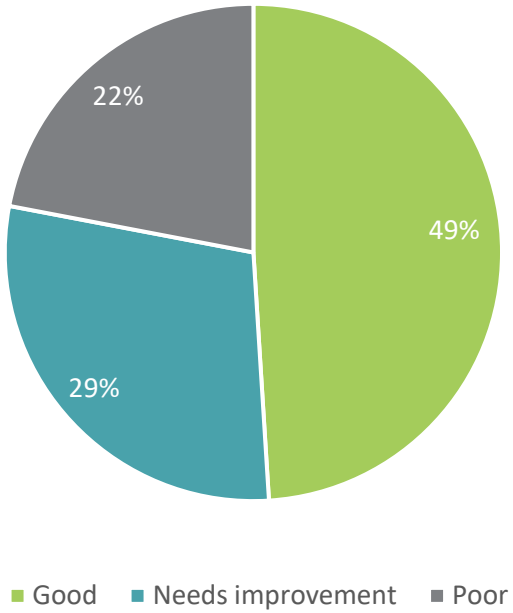
FID evaluates the performance of a website when displaying its content on the client side, while FCP and RT measure the time of information exchange between the server and the client.

* *Denial-of-service attack*

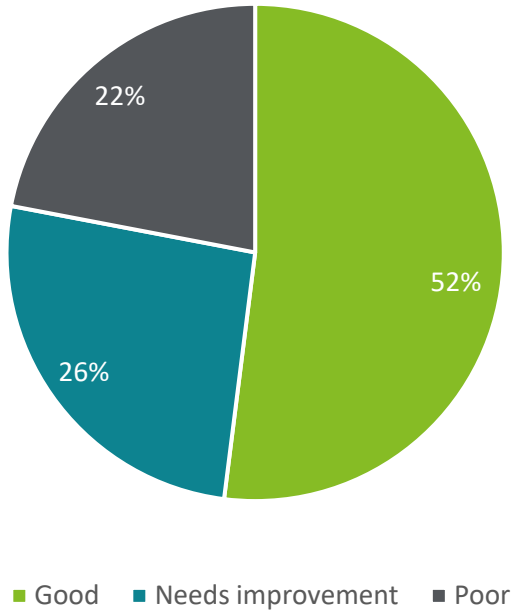
1. Site availability

Summary of all metrics of the “main” category websites

Previous Report results



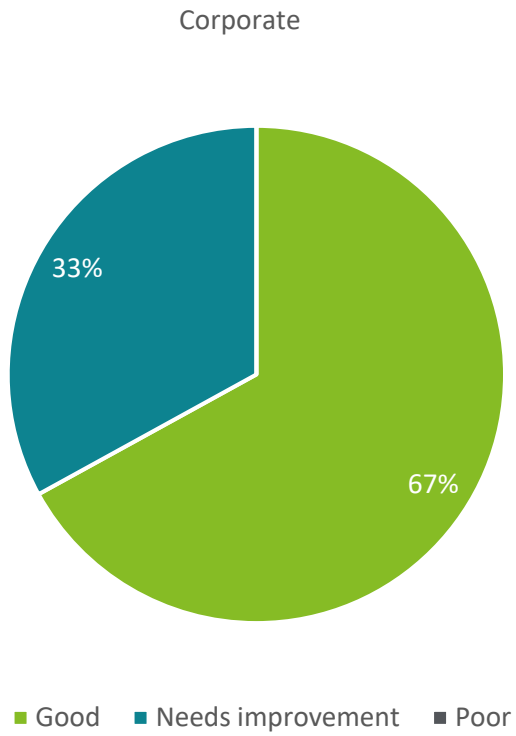
Current Report results

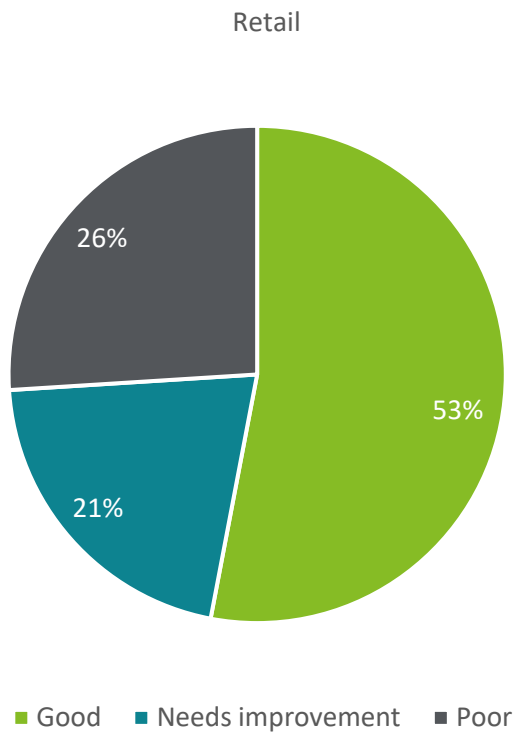


The lack of any real difference between the current result and last year's report can be explained by the margin of error in measurements.

1. Site availability

Summary of all “corporate” and “retail” website metrics





The proximity of the results for the additional categories to the main site results allows us to conclude that over 50% of banks understand the significance of continuous website access. However, it also means that the minority need to improve their performance.

1. Site availability

1.1 First Input Delay

The "First Input Delay" indicator is an important site parameter, forming the so-called "first impression" of website speed. FID evaluates site interactivity and responsiveness by measuring the time it takes for the browser to process the first user input and display the corresponding content. The lower-the-better rule is applied when assessing results.

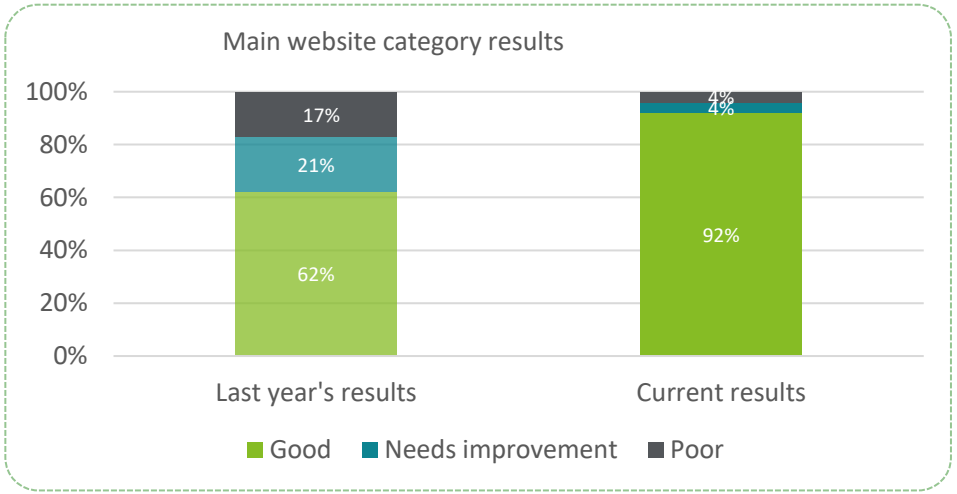
A high FID value can be an indicator of poor website optimization or excessively "heavy" code or content, which can lead to slow website element loading and display on the user side.

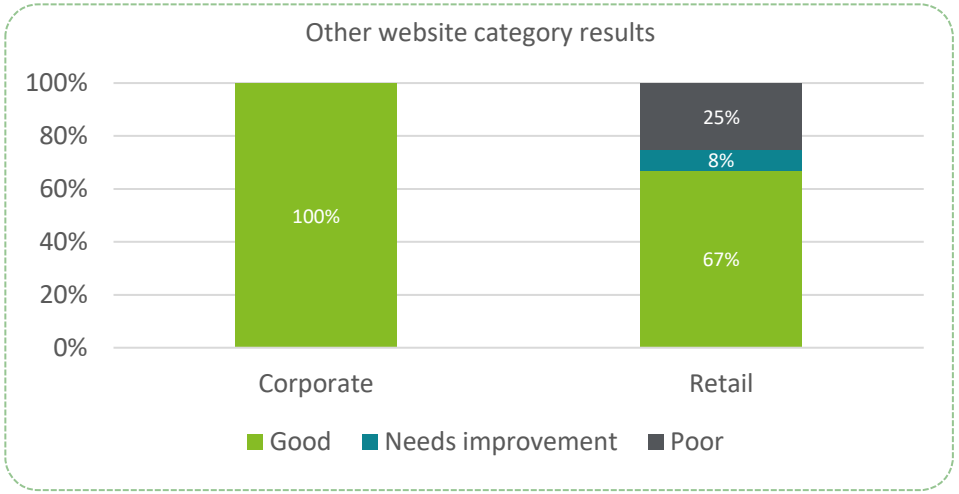
Each result was interpreted by comparing the results obtained according to the following criteria: from 0 to 100 milliseconds – "Good", from 100 to 300 milliseconds – "Needs improvement", over 300 milliseconds – "Poor".

According to these statistics, all three categories performed fairly well. It is clear that banks are serious about receiving a good "first impression" from their users. 92% of the main category banks scored 'Good' and only a small proportion (4% each) were rated 'Poor' and 'Needs Improvement'.

Nevertheless, those falling into these categories need to improve their sites by:

- Breaking long tasks into parts.
- Optimizing the page for interaction readiness.
- Using the Web Worker API.
- Limiting JavaScript execution time.





1. Site availability

1.2 Response time

Website Response Time (RT) represents the time between a user website request and the moment when the first data from the website is received. RT is measured in milliseconds, and the lower-the-better rule is applied when assessing results.

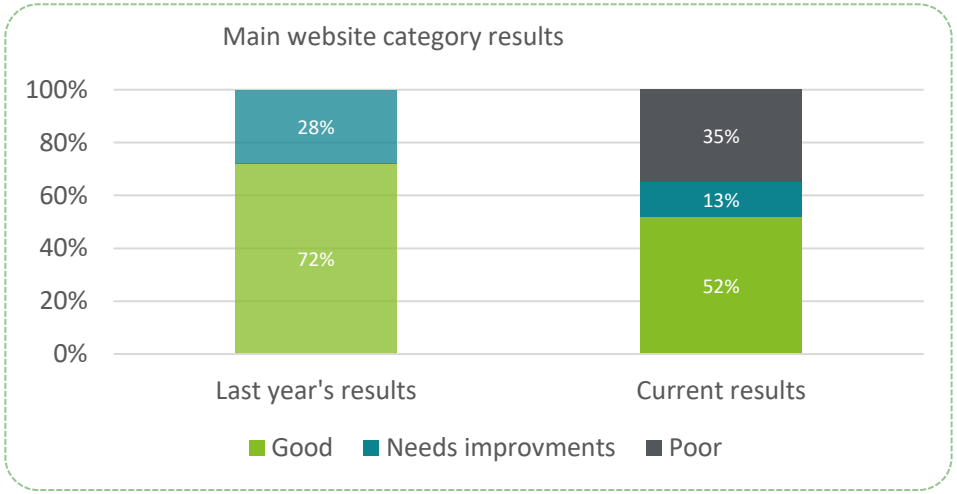
We used the K6 online load testing tool to measure RT values. The testing configuration included 20 virtual users (VUs) from Europe (Germany) who generated a load similar to real users, with five minutes for testing. After the test run, the average response time was calculated from the pools of requests of the 20 VUs within the specified time frame. The average result of all queries during this time was taken as the RT value.

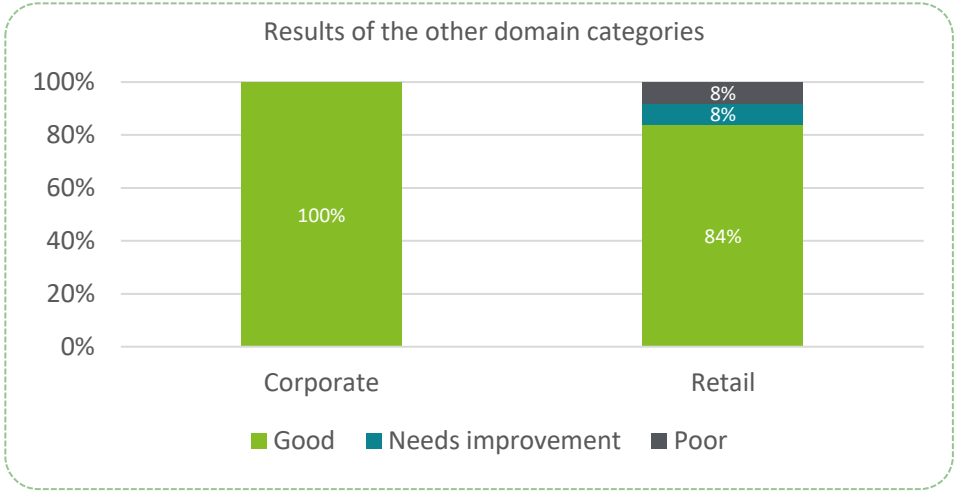
Each result value was interpreted by comparing it with the following indicators: up to 500 milliseconds - "good", 500 to 1000 - "Needs improvement", longer than 1000 milliseconds - "bad".

The results of our analysis of current and previous year RT scores for the main categories showed that 20% of the sites with ‘Good’ results were moved to the 'Needs Improvement' and 'Poor' categories, which is a significant decrease. Also, we noticed that the main sites took more time to respond to queries.

There are quite a few issues that affect RT performance, and they can be improved by:

- Optimizing server application logic so that pages load faster.
- Optimizing server database queries or moving to faster database systems. Database access caching can also be useful.
- In some cases, upgrading server hardware, in terms of more memory or CPU resources, may also help.





1. Site availability

1.3 First Contentful Paint

FCP measures the time it takes for the first website content items to be displayed in a browser window in response to a user request. This allows the user to ensure that the requested resource is available and it handles requests properly. The indicator is measured in milliseconds. Therefore, the rule "the lower the number, the better" applies to results.

We used Google's PageSpeed web resource for testing, and timing values were interpreted using the ranges stipulated by Google's official performance scoring method.

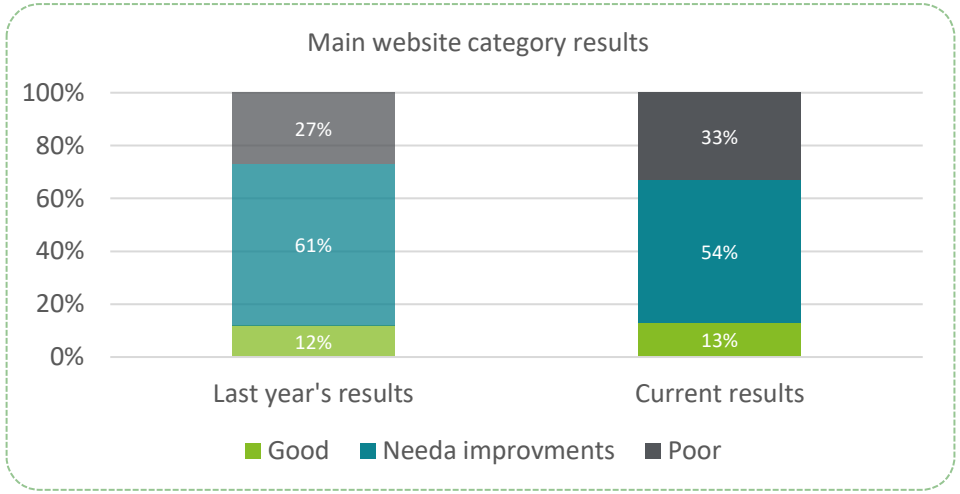
Each result value was interpreted by comparing it to the following: from 0 to 1,800 milliseconds - "Good", from 1,800 to 3,000 milliseconds - "Needs improvement", and over 3,000 milliseconds - "Poor".

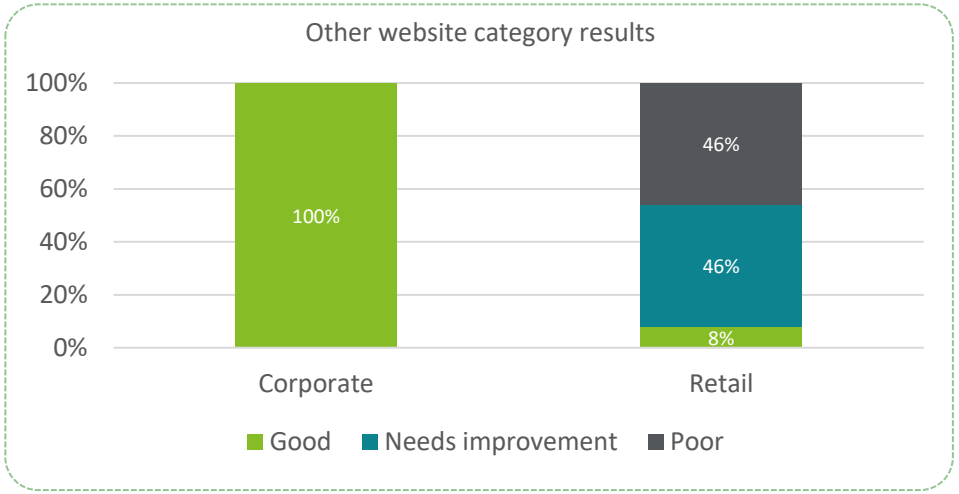
An analysis of FCP results shows that Azerbaijan bank FCP results have remained almost unchanged year-on-year, suggesting that they have not taken any measures to improve the situation.

The results also indicate that Corporate Banking statistics are significantly higher than its Retail business counterpart.

The list of possible improvements to improve this indicator is rather long, so we highlight the key ones below:

- Refuse to use resources blocking content rendering.
- Minimize the use of style sheets (CSS), including exclusions of unused styles.
- Improve page loading speed with pre-connection.

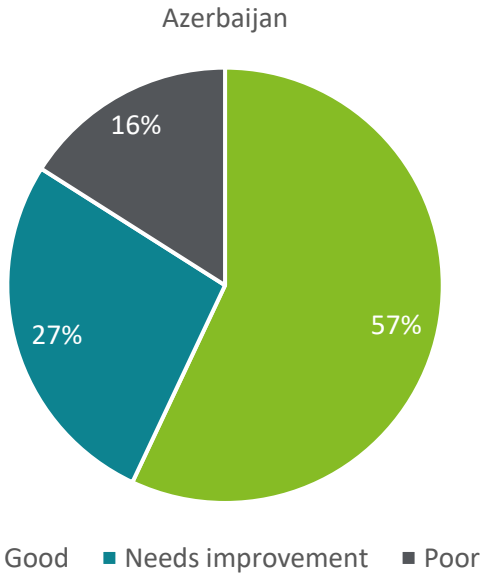


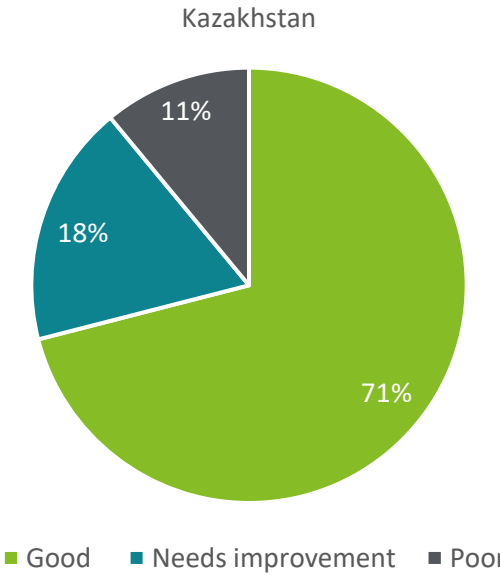


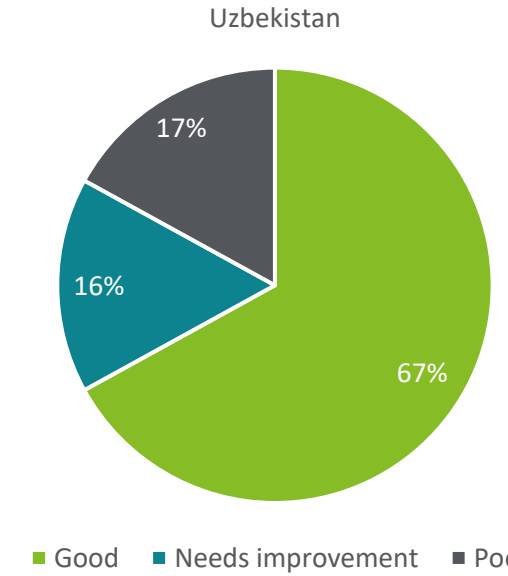
1. Site availability

Conclusion

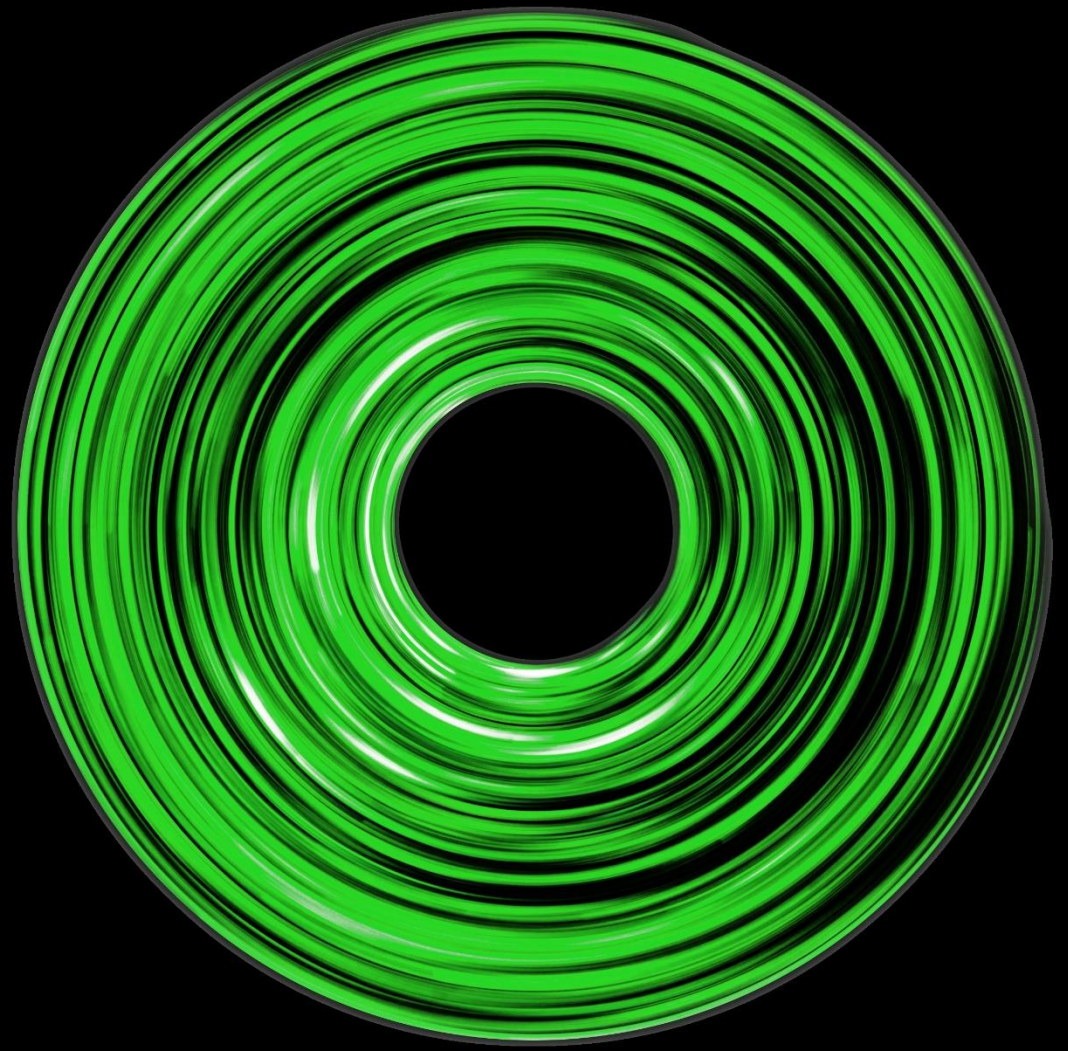
The results of the availability survey across all domain categories indicate that website performance in over half of the banks in Azerbaijan meets security requirements.
The server's first contentful paint parameter had the greatest impact on the decrease in accessibility results. Thus, according to Google, users leave a site if it takes more than three seconds to load, and the server's first contentful paint plays a very important role because it is the first point in the page load timeline when a user can see something on the screen - a fast fcp helps reassure the user that something is happening.
The figures below provide a comparison of generalized accessibility indicators by country:







2. Domain reputation



2. Domain reputation

Domain reputation plays a critical role in trust relationships in cyberspace. Since email providers and search engines began to rely on information from domain reputation providers, this factor has only grown in importance.

Emails sent from domains with low reputation scores or blacklisted by web reputation providers may be flagged as spam by email service providers and their web resources may not show up in search results.

In this section, we present the results of our domain reputation analysis of Azerbaijan banks, which was conducted using three web reputation providers:

- Talosintelligence;
- TrustedSource;
- Barracuda Reputation System.

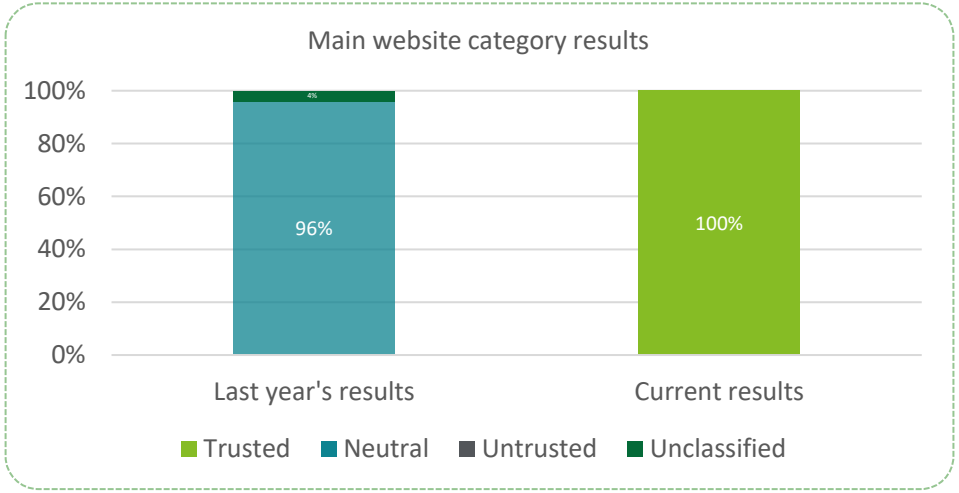
2. Domain reputation

2.1 Talos Intelligence

Talos Intelligence provides domain reputation assessment services from Cisco. The service identifies and correlates threats in real-time using the world's largest threat detection network, covering emails, web queries, malware instances, datasets, endpoint analysis, and network intrusions.

Talos categorizes domain reputations into four groups: Trusted, Neutral, Untrusted, and Unclassified. Before assigning a trusted reputation to a domain, Talos collects substantive positive evidence about it, based on data for the entire domain and all associated IP addresses.

According to our assessment, 0% of banks in Azerbaijan have an untrusted domain. 100% of local bank domains are recognized as Trusted. Overall, the total number of banks with good grades has increased.



100% of additional category websites were recognized as trusted

2. Domain reputation

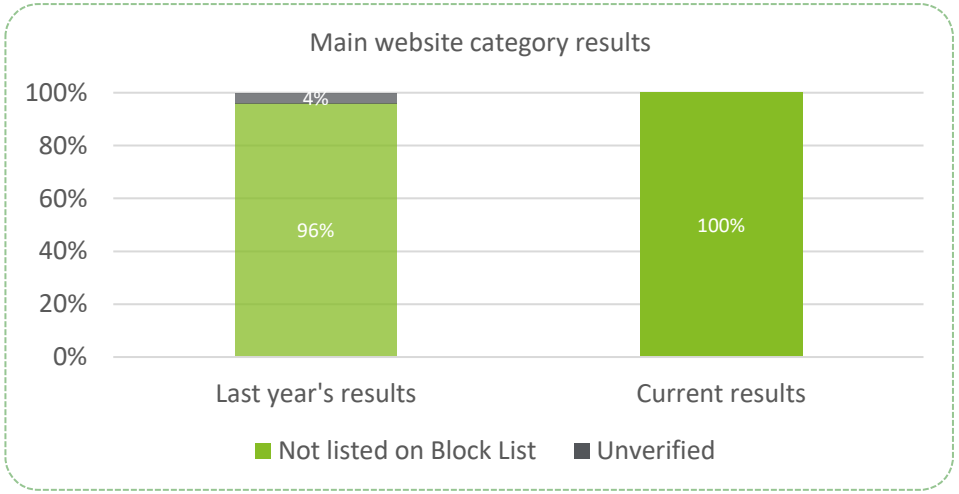
2.2 Barracuda Reputation System

The BRS provides domain reputation information powered by Barracuda Central. It maintains records of the IP addresses of known spammers and senders with good email practices. This data is collected from spam traps and other systems across the Internet. The sending history associated with the IP addresses of all mail servers is analyzed to determine the likelihood that messages from those addresses are legitimate.

This solution relies primarily on the domain reputation verdict provided by the BRS as the first criterion for possibly blocking network attacks sent via email over the Internet and other protocols. Similarly, other Internet solutions and services may also rely on BR's reputation indicators.

The BRS manages a real-time database of IP addresses and domain names with a Blacklisted/Poor and Not Blacklisted/Good reputation for sending valid emails.

According to our assessment, 100% of all main, business, and retail domains of local banks have a good reputation and have not been blacklisted. The overall result has improved by 4% compared to the previous year.



100% of additional category websites were not blacklisted

2. Domain reputation

2.3 TrustedSource

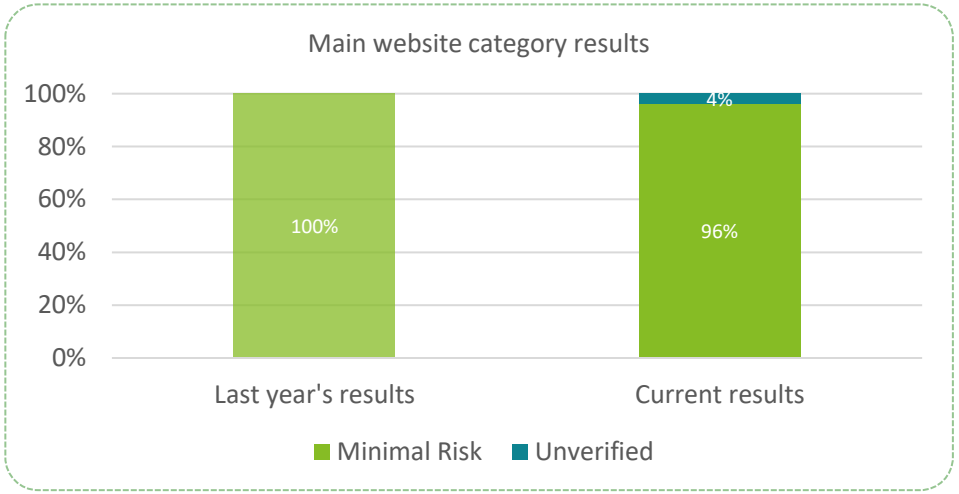
TrustedSource provides domain reputation information powered by McAfee. It rates reputation data and content categories, as well as email, web and other network traffic patterns for IP addresses, domains, and URLs. TrustedSource collects the real-time traffic patterns mentioned above from McAfee's security appliances.

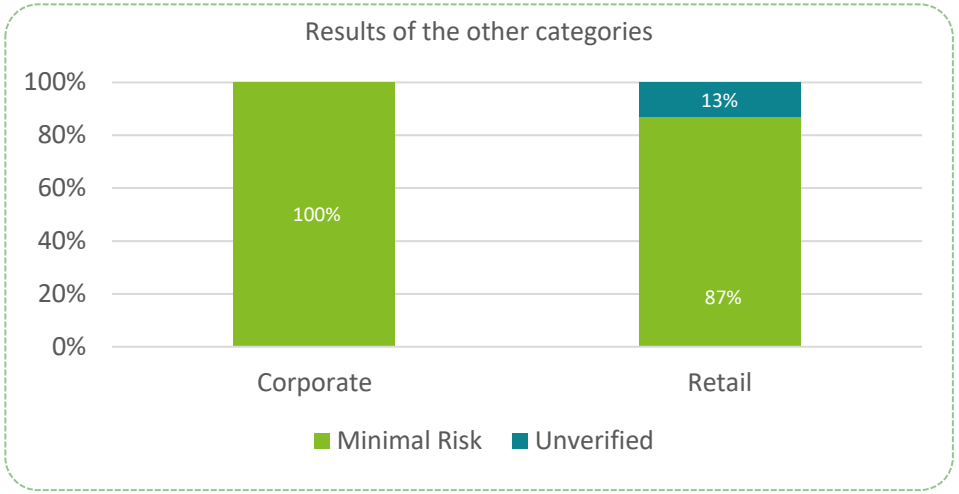
McAfee solutions rely on domain reputation verdicts provided by TrustedSource as the main filter for incoming traffic to block network-based attacks sent via email, web, and other protocols, as well as to reduce unwanted network traffic. Other solutions may also rely on TrustedSource reputation verdicts.

Domain reputation verdicts from TrustedSource rank risks as High, Medium, Minimal, or Unverified. TrustedSource assigns Minimal Risk verdicts to domains for which no suspicious activity is detected during testing. An Unverified reputation means that the domain URL has been referenced in a web or email link before but has not been tested yet.

According to our assessment, 96% of the main domains showed minimal risk. The number has decreased by 4% compared to the previous year's result.

Furthermore, the overall result for business and internet banking domains look satisfactory with percentages of 100% and 87% accordingly.





2. Domain reputation

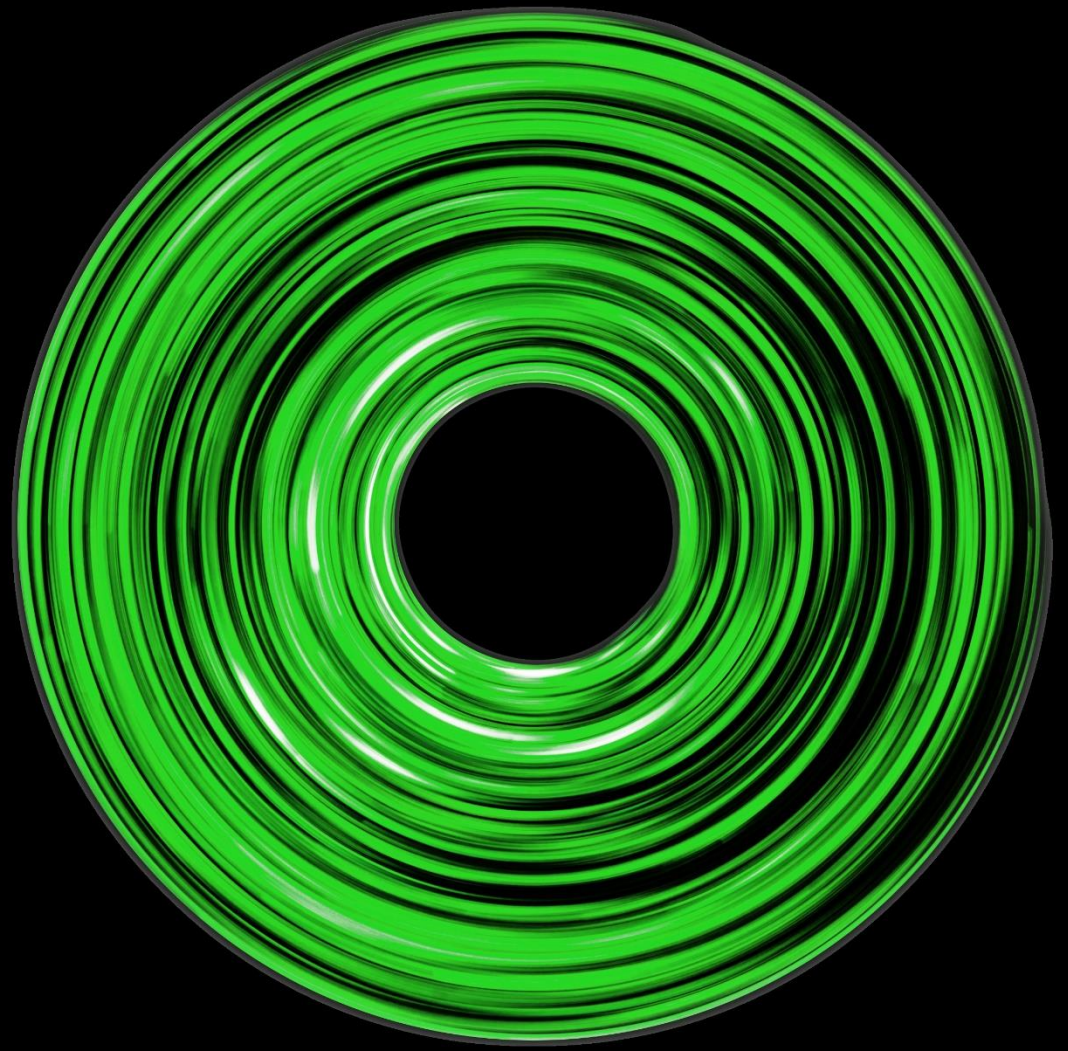
Conclusion

Analysis of the domain reputation of banks in Azerbaijan shows that domain reputation has improved for more websites since the previous assessment. This means that their domains have not been used for spam, spreading viruses or other suspicious activities, or at least they have not appeared in the global-level spotlight and therefore have not been evaluated.

Generalized domain reputation results for all website categories for the three countries:

The reputation of 97% of the Azerbaijan bank websites tested is **Good**	The reputation of 98% of the Kazakhstan bank websites tested is **Good**	The reputation of 98% of the Uzbekistan bank websites tested is **Good**

3. HTTP security



3. HTTP security

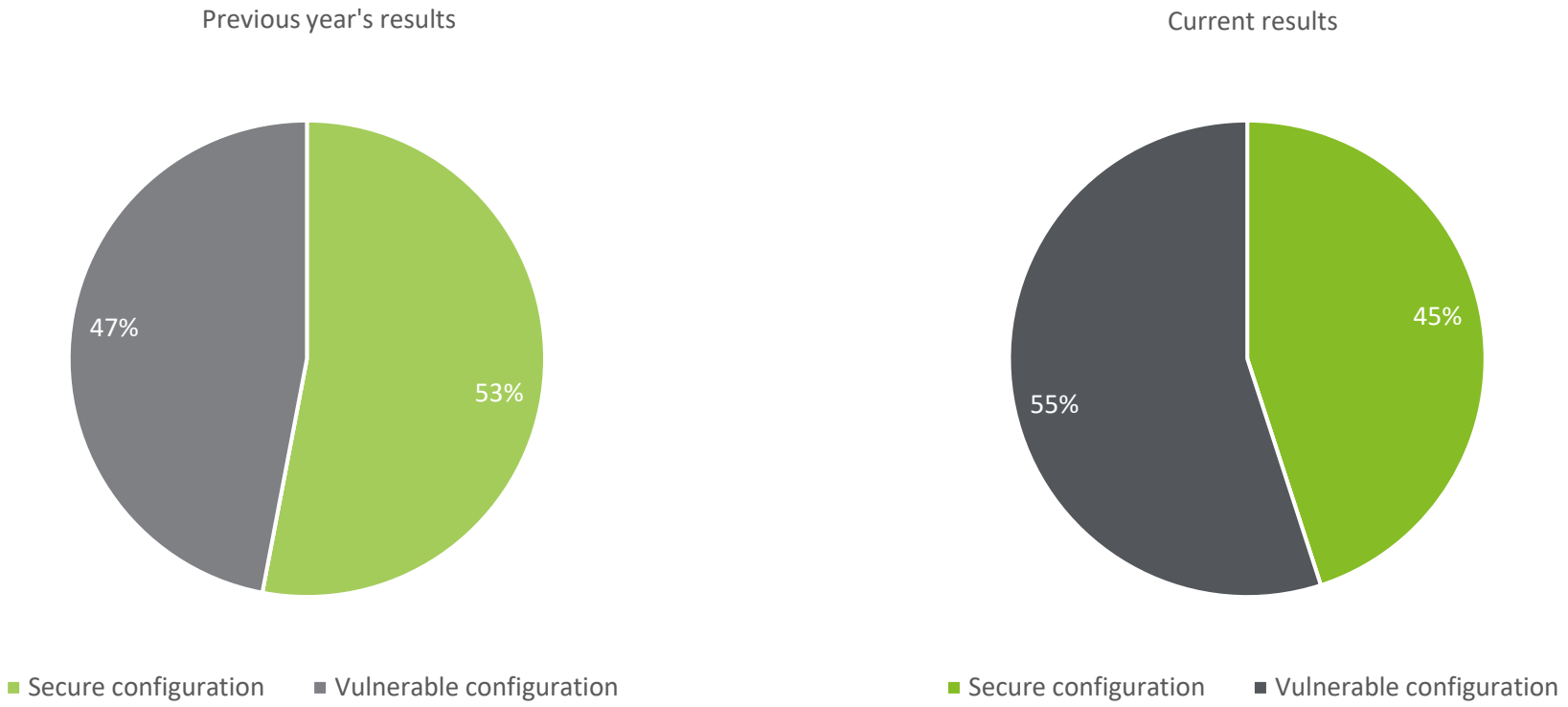
Website security covers a wide range of measures and violating the integrity of just one component may lead to an entire site being hacked. The consequences of these types of incident can be quite devastating, including financial or reputational losses. This is why banks need to ensure full compliance with all cyber-security requirements. Only this approach can minimize the risk of the possible compromise of Internet resource security.

One of the basic methods of protecting Internet site security is the correct configuration of HTTP headers. As part of this review, we analyzed the settings of the following HTTP headers using a publicly available resource - Mozilla Observatory:

- X-Frame-Options
- Content-Security-Policy
- HTTP-Strict-Transport-Security
- X-Content-Type-Options
- X-XSS-Protection
- Set-cookie security flags
- Public-Key-Pins
- X-Powered-CMS
- X-Powered-By
- Server Header

3. HTTP security

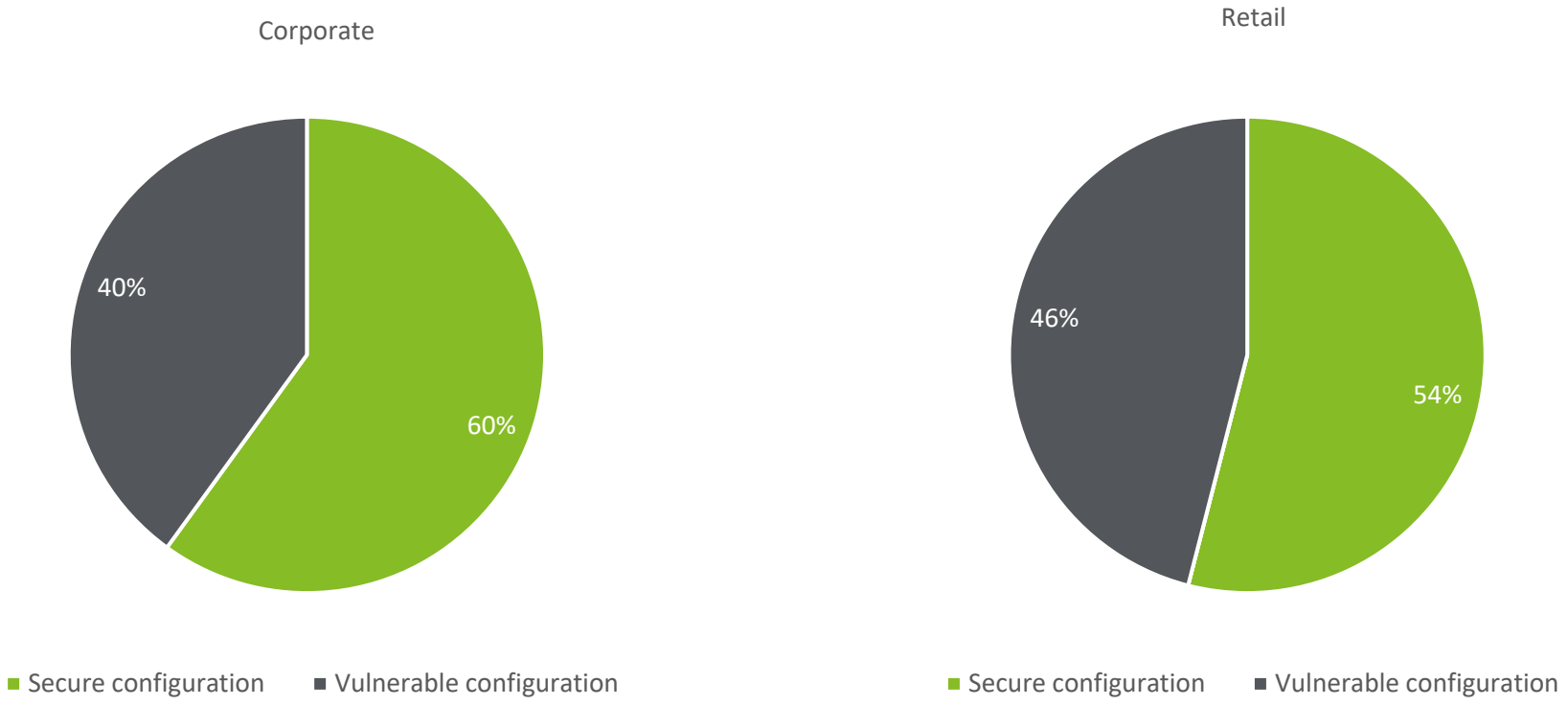
Result of all HTTP headers checked for the "main" website category



This year’s assessment shows that “good” secure HTTP header configuration results dropped 8%. Missing HTTP security headers can lead an unaware user to navigate to an unencrypted version of the web application, which can lead to sensitive data being sent over an unencrypted wire.

3. HTTP security

Result of all HTTP headers for "Corporate" and "Retail" website categories



Analysis of HTTP additional category security settings also shows that more than 50% of banks pay attention to this security category. As such, all remaining banks are recommended to implement appropriate corrective measures.

3. HTTP security

3.1 X-Frame-Options

This header specifies whether a browser is allowed to render a page inside a <frame> or <iframe> tag as part of an HTTP response on a web page. Wrong header settings can be used for clickjacking attacks.

The mechanism of this vulnerability is quite simple: the attacked user assumes that they are interacting with the bank's website, at least outwardly. In reality, the user is interacting with the attacker's resource.

Our assessment found that compared to last year, the results of the main category banks that use headline support have increased by 10%. However, more than a third of banks still do not use it.

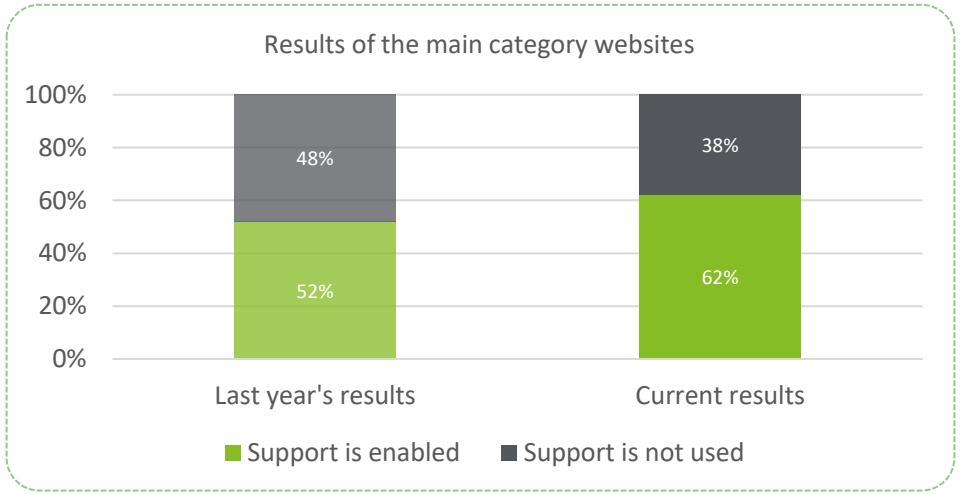
It should be noted that the figure was slightly worse for Retail sites, i.e. 47%, whereas all corporate sites use headline support.

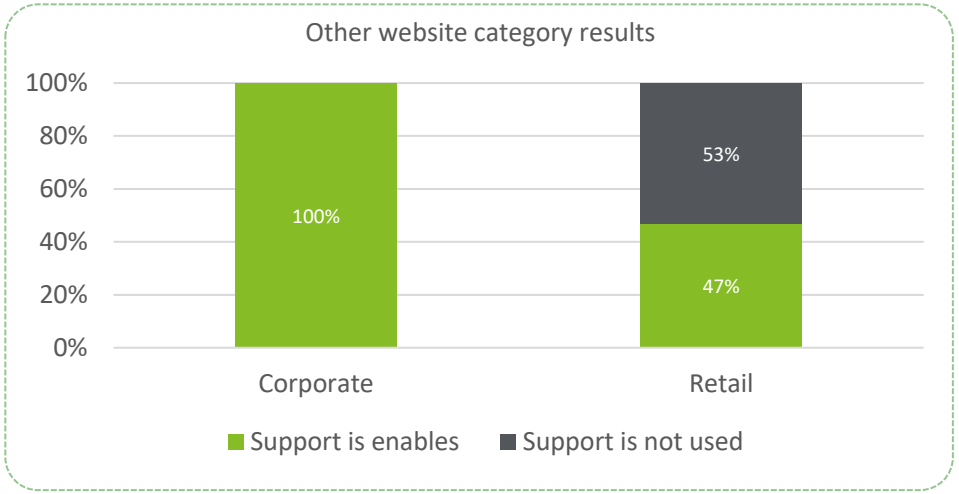
To protect Internet resources from this type of attack HTTP headers need to be configured to three main options:

1. DENY: restricts the current page form being displayed within an iframe;

2. SAMEORIGIN: restricts the ability to display the page only within the current site;

3. ALLOW-FROM URL: allows certain URLs to load site content in an iframe. Note that not all browsers support this option.





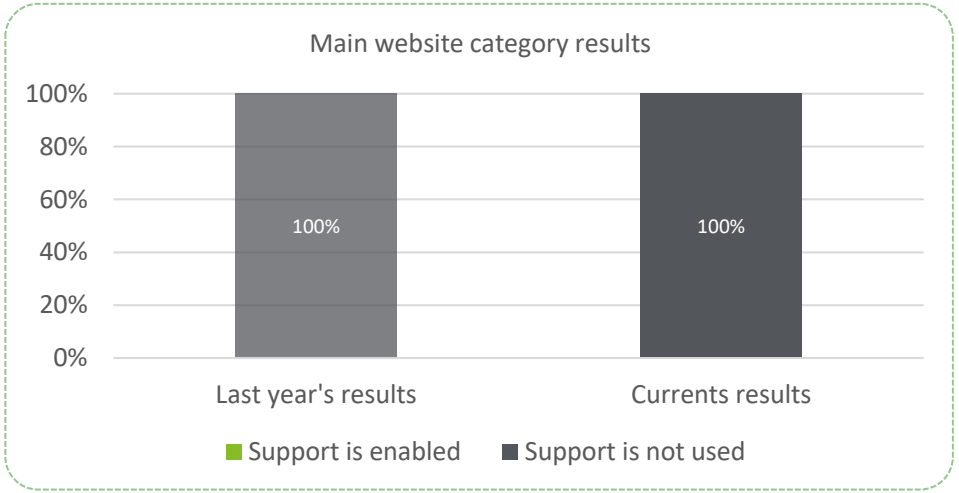
3. HTTP security

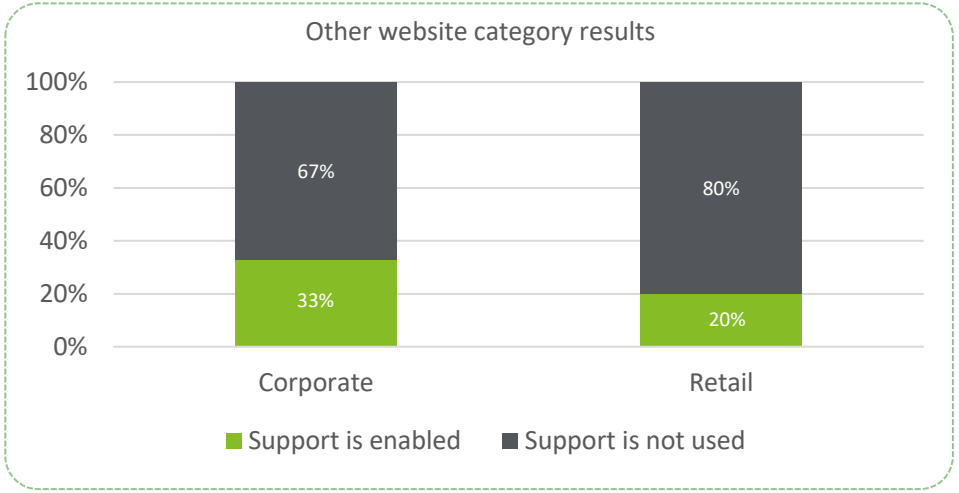
3.2 Content-Security-Policy

CSP headers allow organizations to restrict acceptable website content sources. This header can be considered an additional layer of browser security, which allows the user to limit the browser loading of such resources as JavaScript, CSS, and many others. CSP helps in loading page elements from a predefined source, which allows the user to detect and prevent attacks like XSS, Formjacking, and SQL Injection.

CSP uses the "white list" principle to define the rules, allowing the user to define permissible resources and prevent others from being used. Also, the use of CSP is very important because it can provide a way to obtain information about the occurrence of XSS attacks quickly. When using the "report-url" option, the browsers of both the attacker and victim will send appropriate notifications to the URL as defined by the resource administrator.
According to our assessment, the results are the same as the previous year's. 100% of the main local bank domains do not use CSP headers as part of their web server response. Business category domains have a 13% more secure web response compared to Retail category domains.

Also, the study indicates that administrators generally prefer to use a different variant of this header - X-Content-Security-Policy. It should be noted that the combined use of these headers can lead to the incorrect display of site content in some browsers. Nevertheless, we recommend using Content-Security-Policy instead of the outdated X-Content-Security-Policy.





3. HTTP security

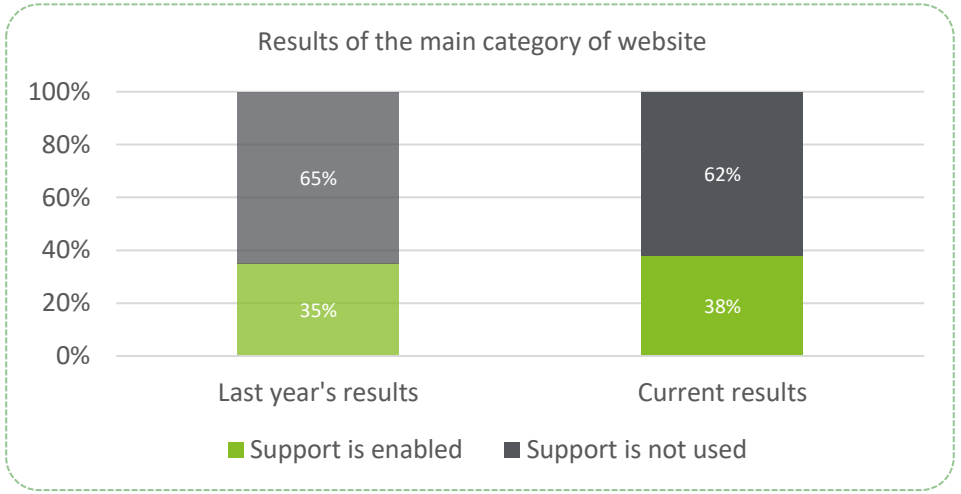
3.3 X-Content-Type-Options

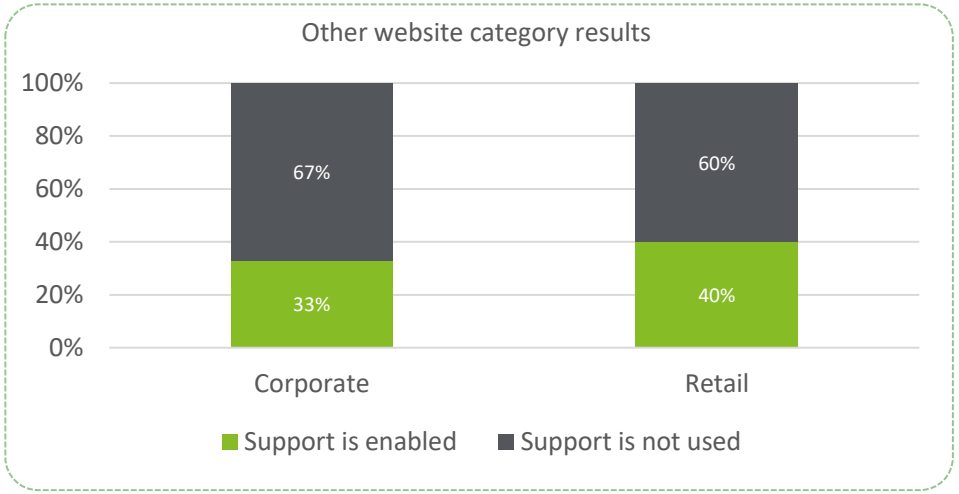
Any HTTP content should include META data about its type so the browser knows what to do with specific content. For example, if the content type header is an image, the browser will know to show it, while if it is HTML it will render the markup and execute any JavaScript code.

However, content type is optional. Web developers sometimes do not use it, which means that browsers must determine what type of content type they are using. For this reason, browsers have had to implement “sniffing” techniques to detect the content type when content type headers are not served.

The analysis shows that in 38% of cases for the main site category, banks use the X-Content-Type-Options header. Compared to the previous year’s results, main category performance improved by 3 percentage points. 40% of Retail domains feature the header while the result for business domains is only 33%.

To avoid serious security issues, we recommend adding the X-Content-Type-Option nosniff line to the HTTP header to prevent Internet browsers from deciding on content by sniffing the MIME Type. Adding this line also enables Cross-Origin Read Blocking (CORB) protection for HTML, TXT, JSON, and XML files (excluding SVG image/svg+xml).





3. HTTP security

3.4 HTTP-Strict-Transport-Security

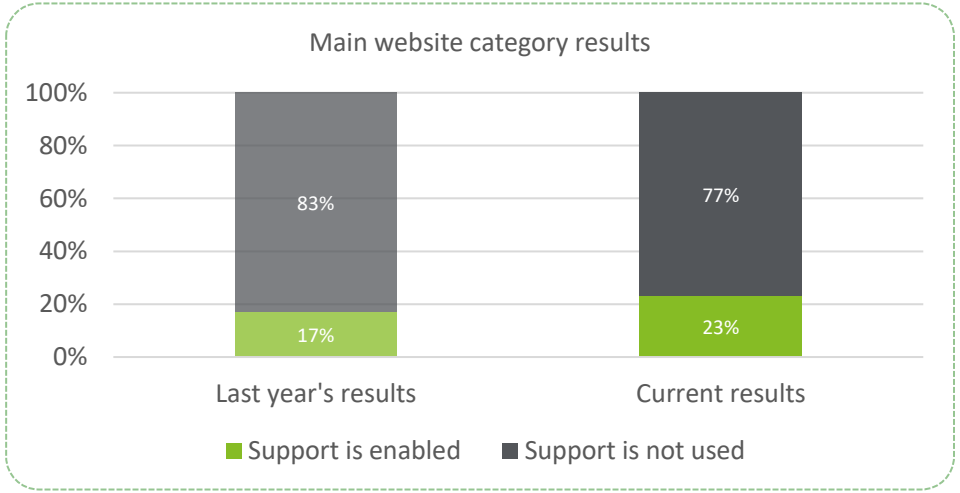
HTTP-Strict-Transport-Security (HSTS) headers force all site users to work over secure HTTPS, without allowing any call to pass content over an insecure HTTP. It is intended to prevent man-in-the-middle attacks.

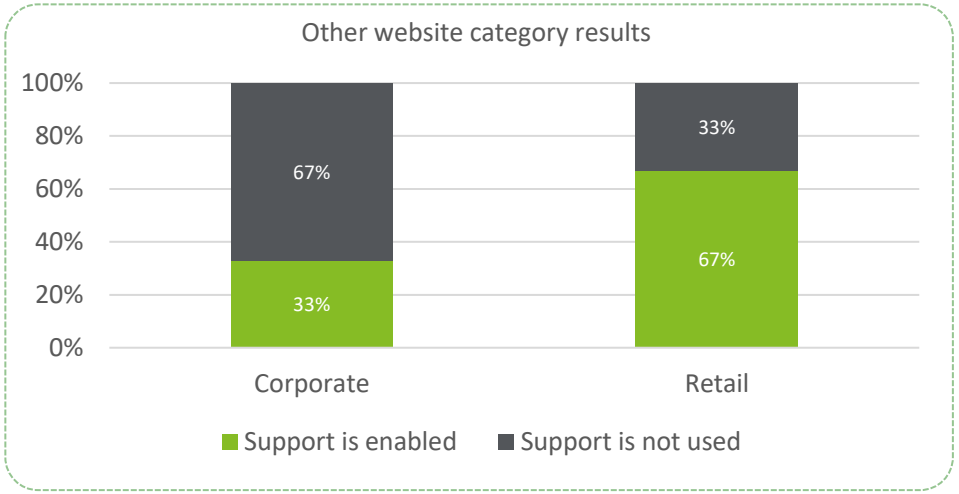
Let's say a website user, or a potential or current bank customer accesses a site via a public Wi-Fi. Passwords and other confidential information in these networks are often available to intruders. Nothing prevents the latter from intercepting confidential information transmitted in the clear by connecting to that Wi-Fi network.

Another way in which an attacker using a 301 or 302 redirect instruction to switch existing session from HTTP to encrypted HTTPS without the final URL present within HSTS. If succeed he can intercept network traffic sent between the user and the website over insecure HTTP. As a result, an attacker avoids SSL encryption of traffic and can intercept personal data or even obtain account credentials.

Even though the main bank sites have showed a 6% improvement compared to the previous year, survey results highlight that a significant number of banks still do not pay attention to protection against the above types of attack.

We recommend activating HSTS use as it will force browsers to load the protected version of the site and ignore any calls or redirect requests to load the site using the HTTP protocol. This closes the redirection vulnerability that exists when using 301 and 302 Redirect.





3. HTTP security

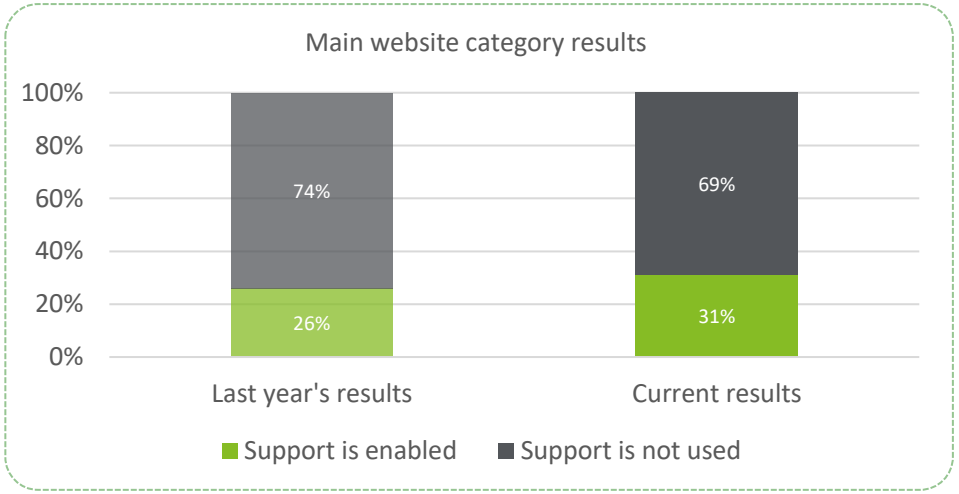
3.5 X-XSS-Protection

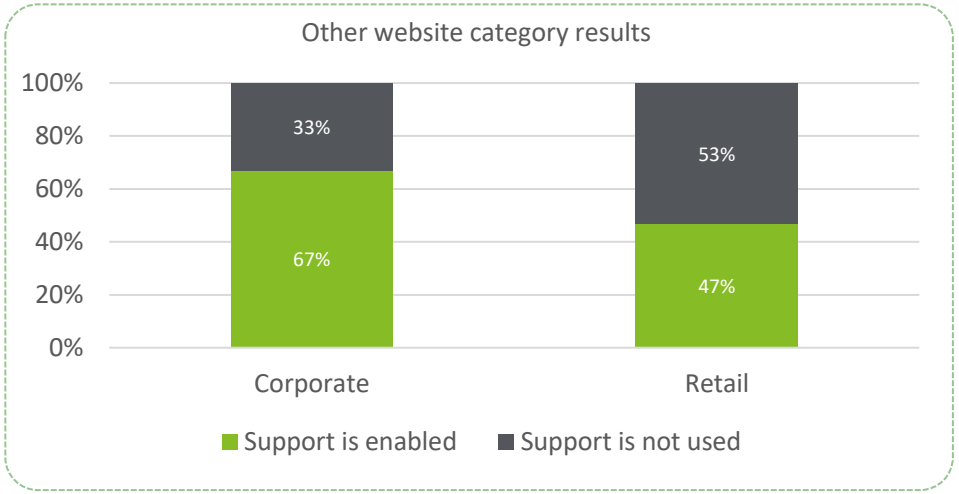
The X-XSS-Protection header is designed to enable a filter against cross-site scripting (XSS) attacks built into modern web browsers. The filter is supported by Internet Explorer version 8+, Chrome, and Safari. It is usually enabled by default, but use in site headers will force its activation. This is especially important in cases where the user has disabled the browser feature themselves. As a result, turning on XSS protection will instruct a browser to block responses if a malicious script has been inserted from user input. If this protection measure is disabled, the malicious script can access the cookie content, session tokens, and other sensitive user information.

According to our review, the overall result has improved 5% on the previous year's assessment. However, still only 31% of local bank main domains have an X-XSS-Protection header in their server response, while 69% do not use the feature at all.

Business domains show the highest results (67%) among all three domain sections.

We recommend that bank site administrators force the use of the X-XSS-Protection header.





3. HTTP security

3.6 Set-cookie security flags

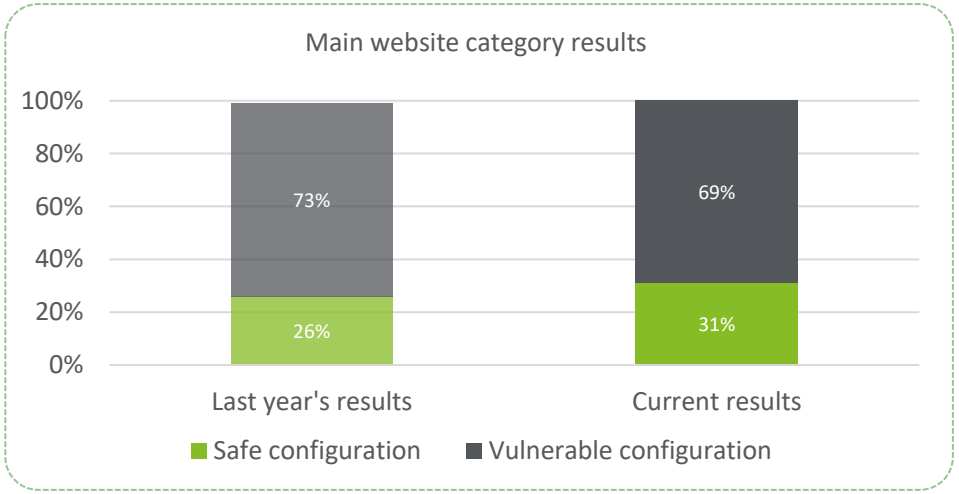
Web applications follow user sessions via a session ID. The value is transmitted to the user with HTTP Set-Cookie header information. Internet browsers retain this value and automatically add it to each HTTP request created as long as the stored cookie remains valid.

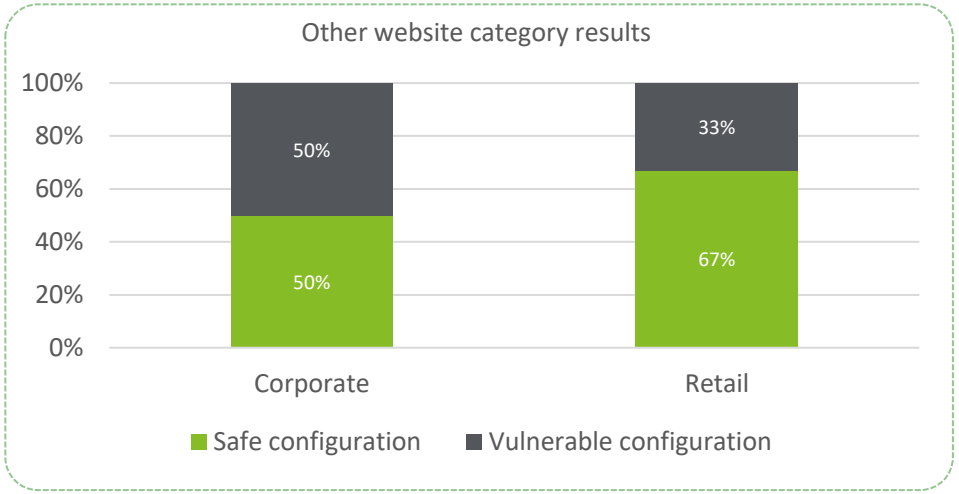
While this is useful, it is important to understand which specific cookie values are important for security purposes. For example, values containing a user ID or session ID should only be used in a secure HTTPS request. Of course, there may be exceptions, but only in extreme cases.

Cookie information can be stolen using JavaScript through attacks such as XSS, which can be protected against using the HttpOnly and secure flags. This will help prevent the theft of information contained in the cookie and minimize the potential risk.

According to our assessment, 31% of local banks use secure flags, while 69% do not. Half of all other category banking sites, both Corporate and Retail, support secure cookie settings. And even though the main site share has increased by 5%, a substantial section of the banks are still recommended to activate the header.

We recommend that site owners activate the HttpOnly and secure flags. Their use in generating a cookie helps mitigate the risk of client-side script accessing the protected cookie.





3. HTTP security

3.7 Public-Key-Pins

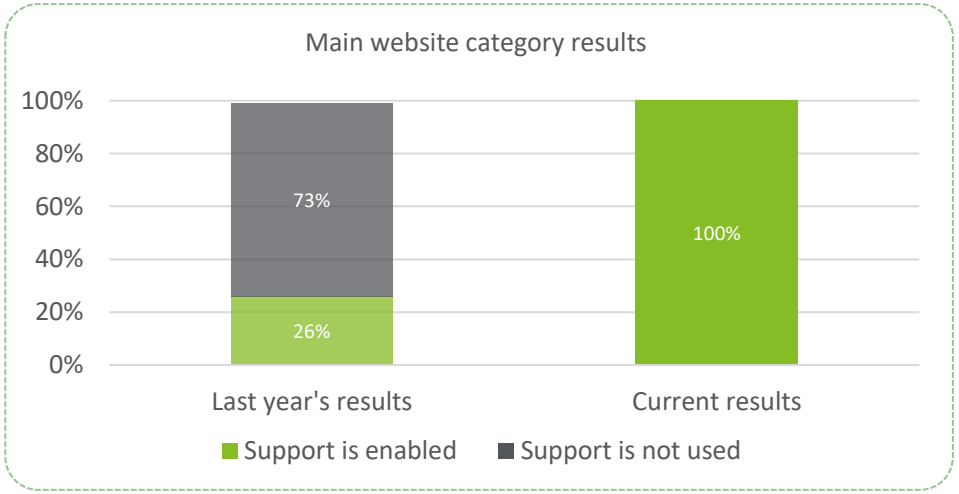
This header instructs the Internet browser to remember the SSL certificate used by the web server. These types of certificate contain information such as site name, certificate validity period, and the length of cryptographic keys used. Certificates also contain additional information such as the name of the Certificate Authority (CA). When sending public key information to clients, the browser verifies website authenticity. To do this, it checks with the CA, which is a trusted party that issues web server certificates.

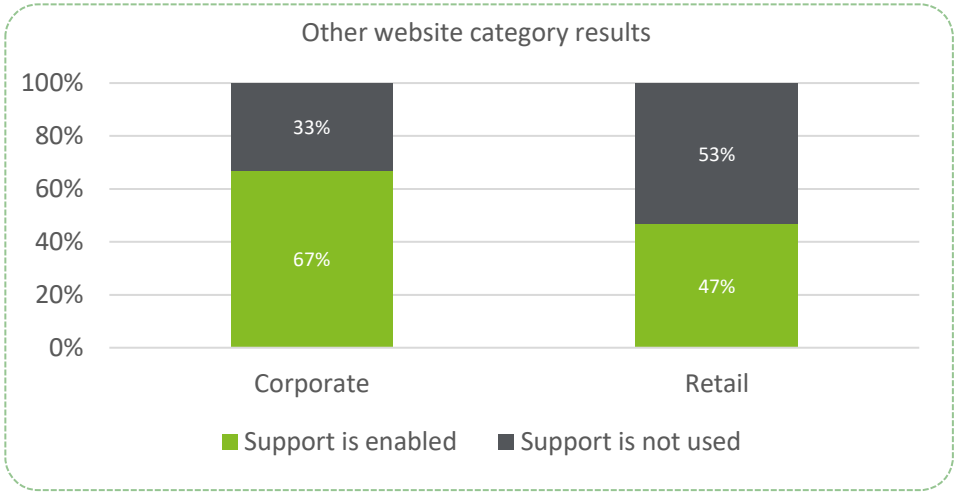
As a result, the user's web browser will not accept certificates with other public keys when subsequently interacting with the site. This is intended to help prevent attacks on users with forged certificates, for example in cases where the CA that issued the certificate has been compromised or hacked to issue forged certificates.

The study shows that banks tend to be prudent and use the header in 100% of cases for the main website category.

In the Corporate and Retail categories, 33% and 53% of banks do not yet use this header.

To avoid serious security issues, we recommend applying HTTP Public Key Pinning (HPKP), which should allow HTTPS websites to resist impersonation by attackers using incorrectly issued or otherwise fraudulent digital certificates.





3. HTTP security

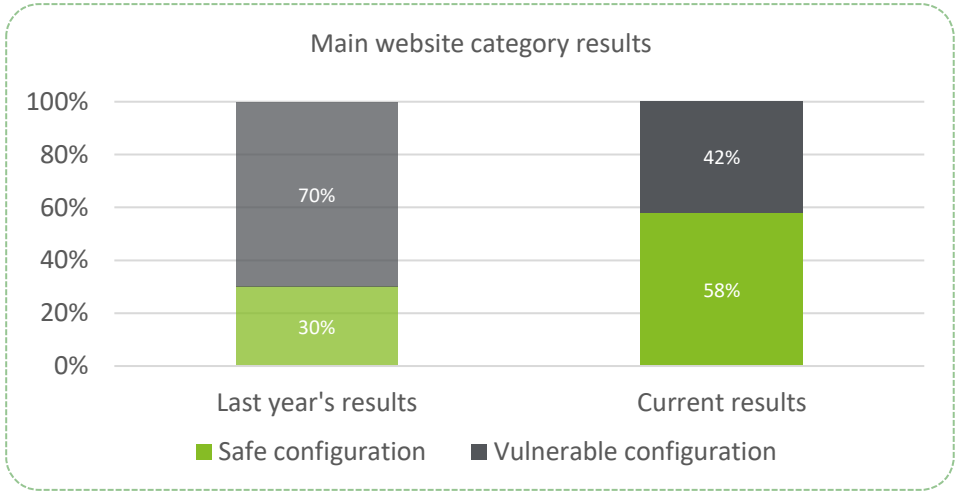
3.8 X-Powered-By

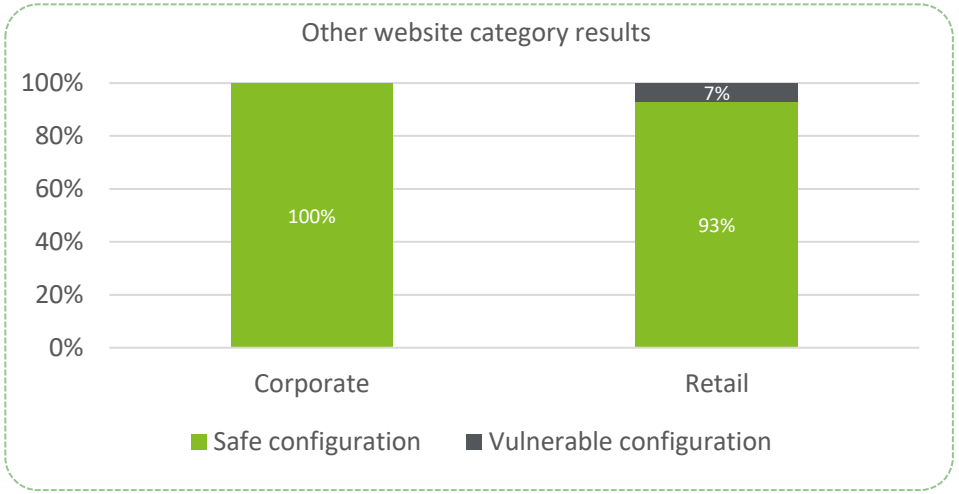
The X-Powered-By header contains information about the technology used by the web server.

This type of information is not particularly dangerous, as long as server software is updated regularly. However, if possible, it is better to hide the name and version. Failure to do so may reduce the time it takes for attackers to gather information and determine subsequent attack vectors.

Our assessment shows that the percentage of the main bank domains that contain default values for the X-Powered-By header increased by 28% compared to the previous year's assessment.

The assessment registered only a 7% difference between Business and Retail domains.





3. HTTP security

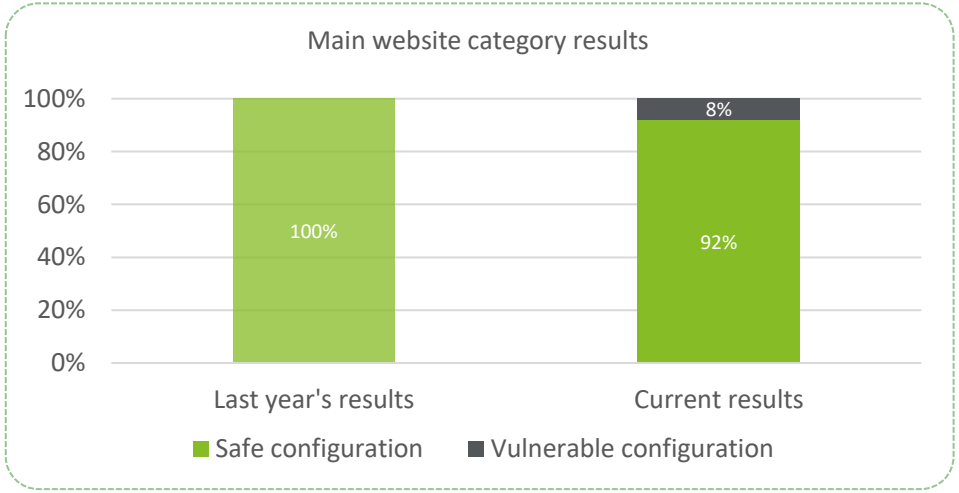
3.9 X-Powered-CMS

The header X-Powered-CMS contains the name and version of the Content Management System (CMS) used to form a website response, such as Bitrix or Express.

This type of information is not particularly dangerous by itself, particularly if server software is updated regularly. However, it is better to hide technology names and versions. Failure to do so may reduce the time it takes for attackers to gather information and determine subsequent attack vectors.

As research shows, banks are critical about hiding this information for the Corporate and Retail website.

In the main category, however, results show that the percentage of domains with X-Powered-CMS has fallen 8% compared to the previous year's results.



100% of additional category websites apply X-Powered-CMS

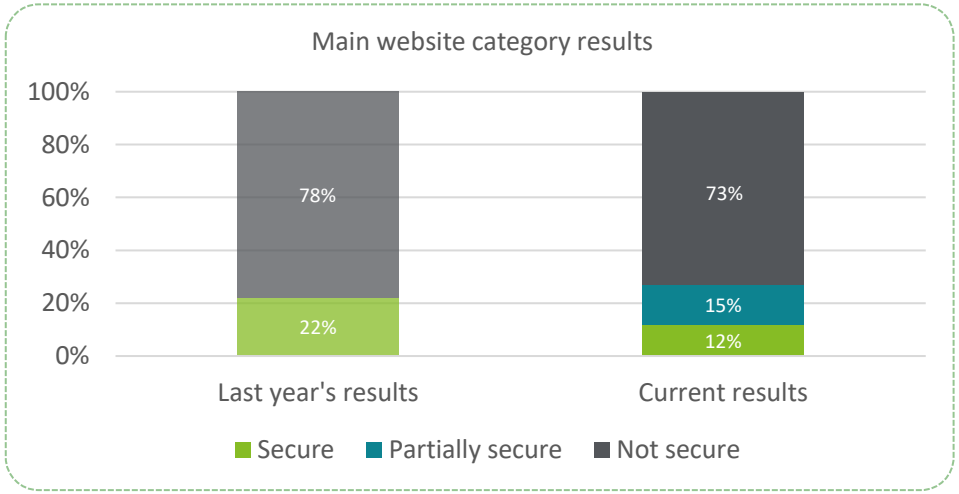
3. HTTP security

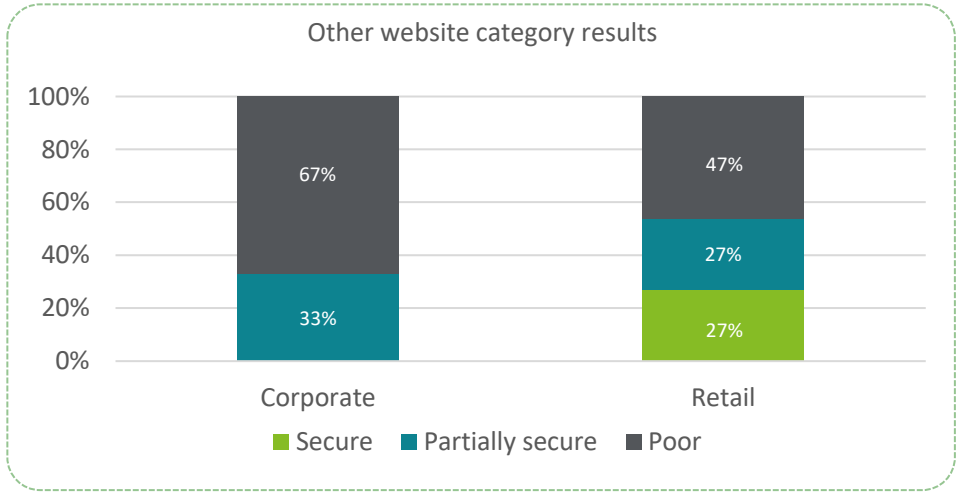
3.10 Server Header

The server header provides a response containing information about the software used by the server to process requests. Common values include nginx/x.x.x, Apache/x.x.x and Microsoft-IIS/x.x.

Similar to the previous two headers, this type of information is not particularly dangerous, provided server software is updated regularly. However, if possible, it is better to hide the name and version of the software used by the server. Failure to do so may reduce the time it takes for attackers to gather information and determine subsequent attack vectors.

Compared to last year, the main category registered a 10% security rating decline. The Corporate and Retail categories also return low scores of 0% and 27%, respectively.





3. HTTP security

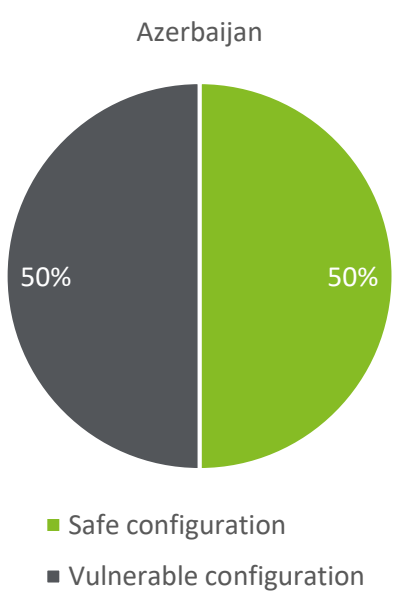
Conclusions

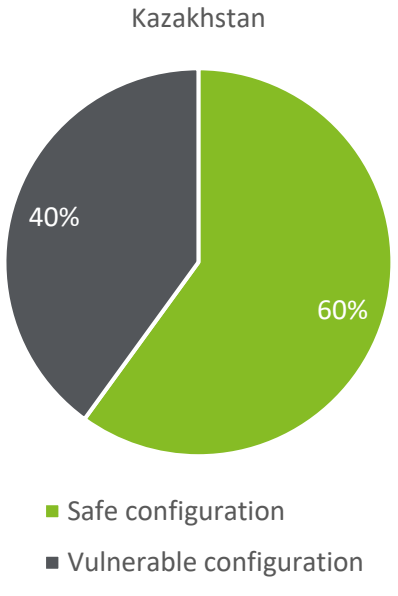
Setting up and maintaining website security is a complex task that includes several areas, and an integrity breach of any of them could be fatal for the entire application and the corresponding data.

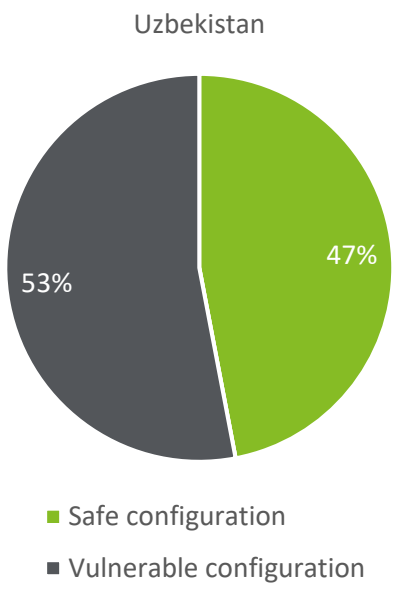
HTTP headers are a good starting point for secure websites, especially considering that most of them are fairly easy to implement in practice. By complying with HTTP security best practices, headers provide an additional layer of security on top of any other security measures.

The HTTP security results for all three categories in Azerbaijan banks showed that in 50% of cases, this security measure is used actively. However, we still recommend the other half take advantage of begin to use them.

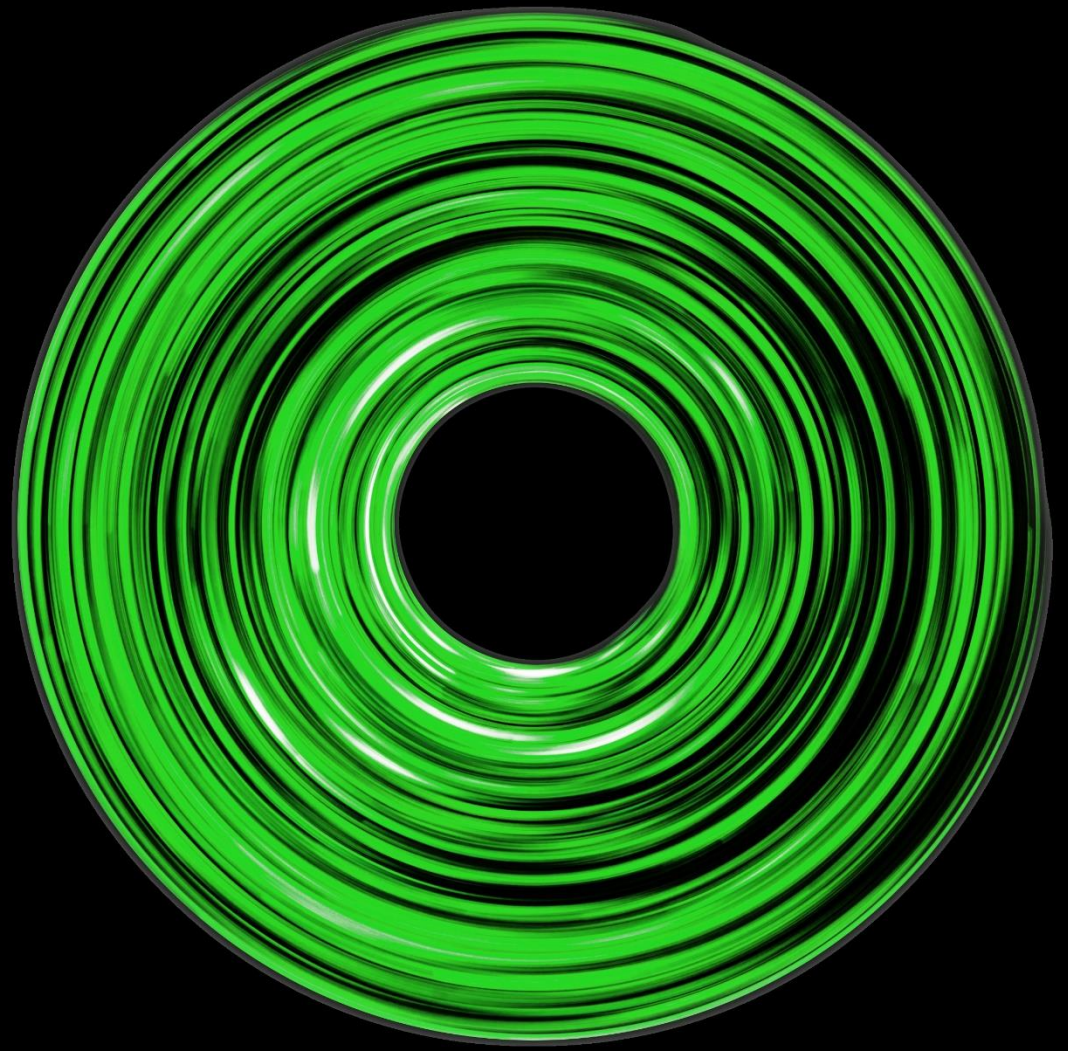
Summary of HTTP security results for all domain categories by country:





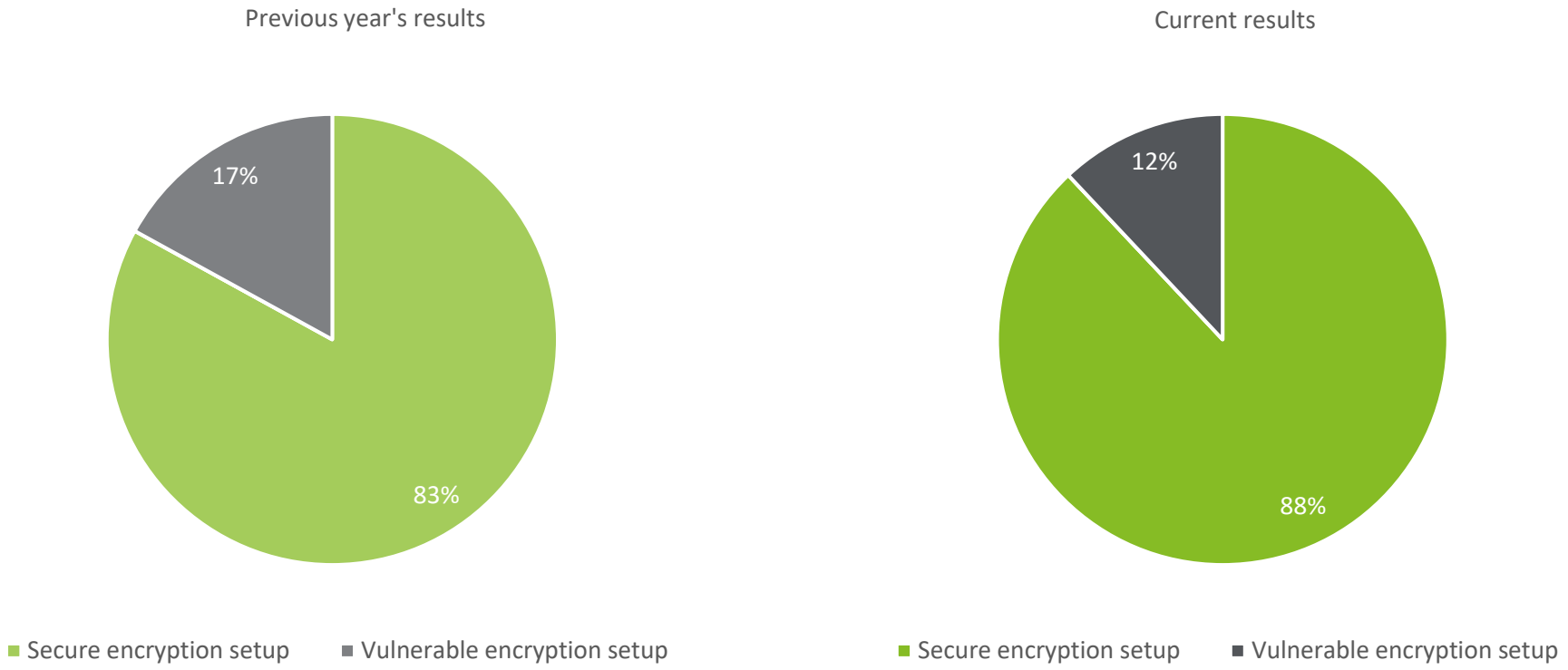


4. Traffic security



4. Traffic security

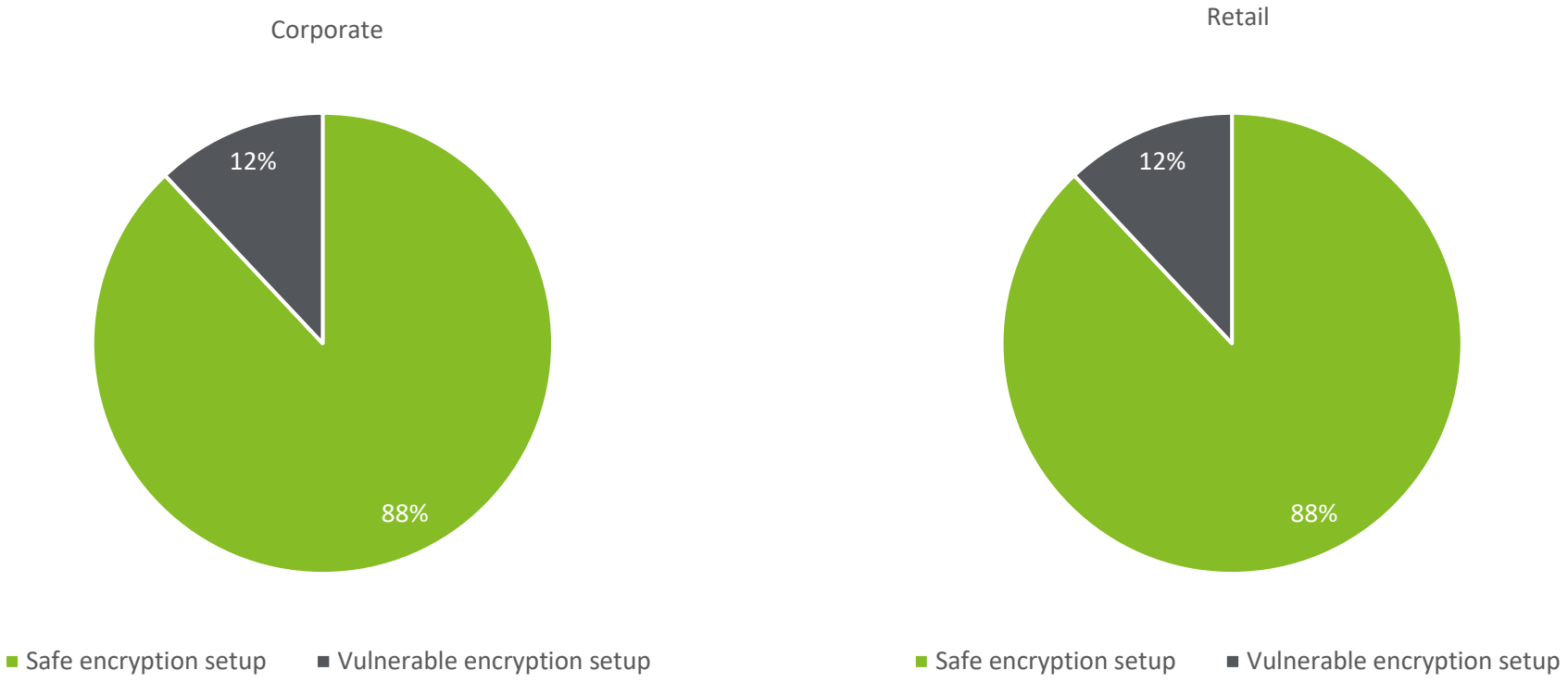
Summarized traffic security results for the "main" website category



The number of banks that have improved traffic security has increased since the publication of the previous Report.

4. Traffic security

Summarized result of traffic security for the "Corporate" and "Retail" website categories



As can be seen from the chart, regardless of the website category, most banks ensure traffic security on their sites

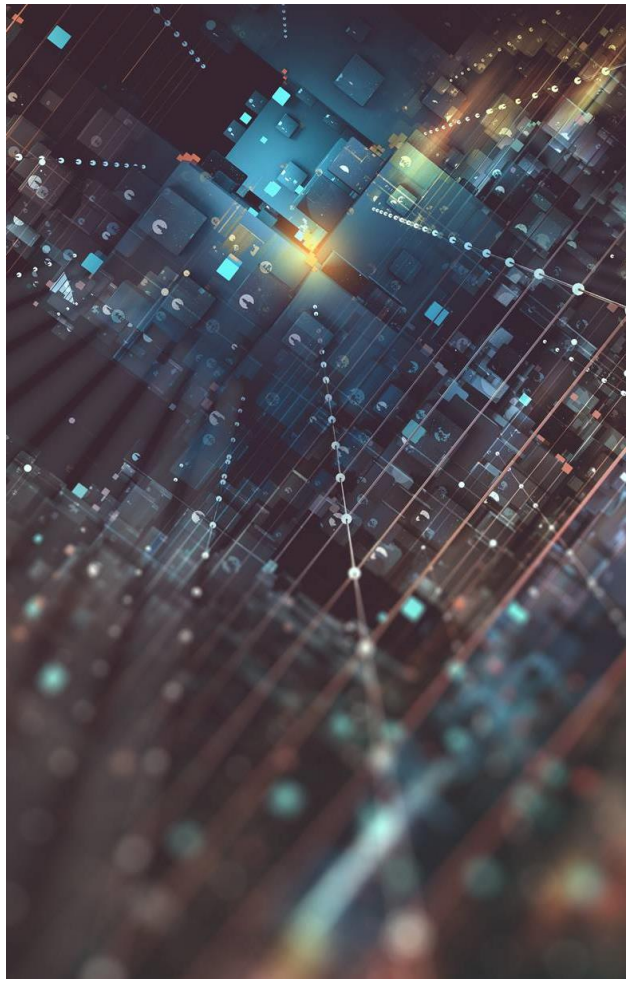
4. Traffic security

Today, both consumers and businesses choose partner services based on HTTPS, which is a secure version of the common HTTP protocol for accessing web resources. HTTPS encrypts data using the Transport Layer Security (TLS) protocol and its previous version, Secure Sockets Layer (SSL). These cryptographic protocols are the most popular methods for providing secure communication on the Internet.

For an SSL/TLS connection, a digital certificate must be installed on the server, proving website authenticity and its owner. This is necessary to ensure that the user is visiting a genuine resource, and not a fake page created by an attacker.

Using the SSLlabs public resource, web servers were tested for the following vulnerabilities:

- Weak DH parameters
- BEAST attack
- Heartbleed
- Ticketbleed
- OpenSSL CCS vuln. (CVE-2014-0224)
- OpenSSL Padding Oracle vuln. (CVE-2016-2107)
- ROBOT
- GOLDENDOODLE
- OpenSSL 0-Length (CVE-2019-1559)
- POODLE
- FREAK attack
- DROWN attack
- TLS 1.1, TLS 1.0 support
- SSL 3.0, SSL 2.0 support
- RC4 support

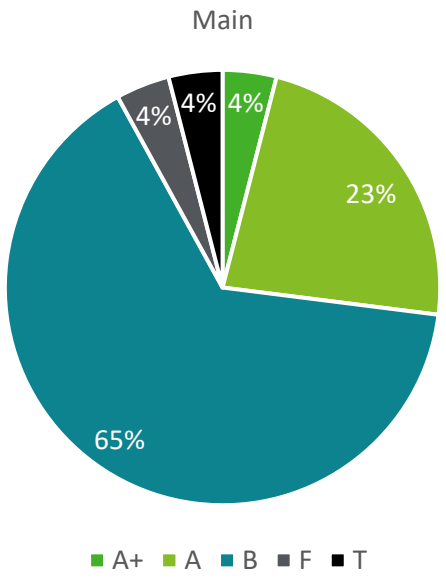


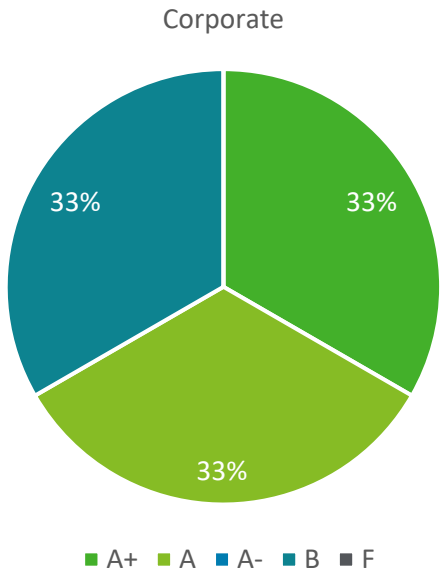
4. Traffic security

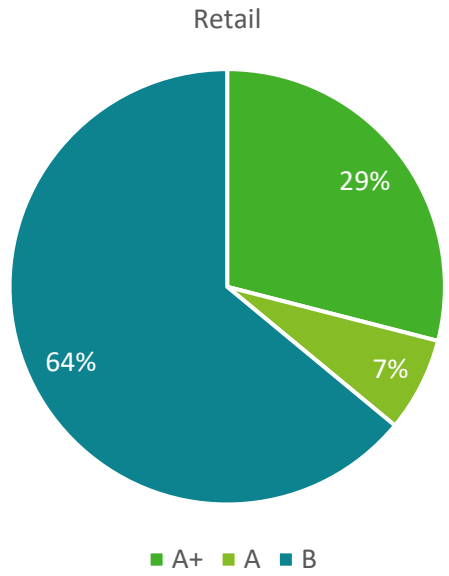
4.1 SSL Labs

Warnings and restrictions built into browsers have made it easier to determine how strong a site or service's encryption is. We used the Qualys SSL Labs service to evaluate these parameters and the rating applied in descending order is A +, A, B, C, and F. SSL Labs can also assign a "T" rating to domains whose certificates turned out to be unreliable.

The best situation with certificates is observed for the main category sites, followed by Retail and then Corporate category sites. In 4% of cases, certificates are recognized as unreliable.







4. Traffic security

4.2 Weak Diffie-Hellman parameters

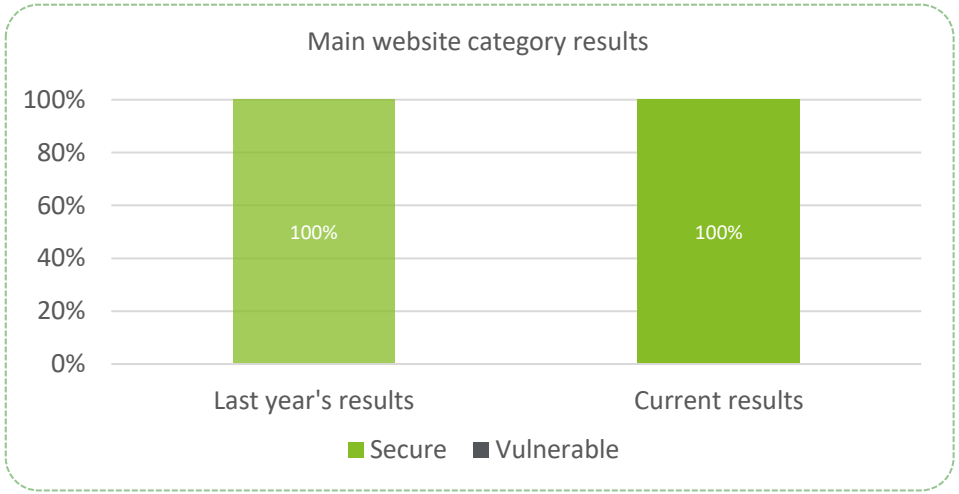
Secure encrypted communication between two parties requires a prior exchange of keys over a secure physical channel, such as paper key lists sent by a trusted courier. The Diffie-Hellman key exchange method allows two parties who do not know each other to exchange a secret key over an unsecured communication channel. This key can then be used to encrypt subsequent messages using a symmetric key encryption algorithm.

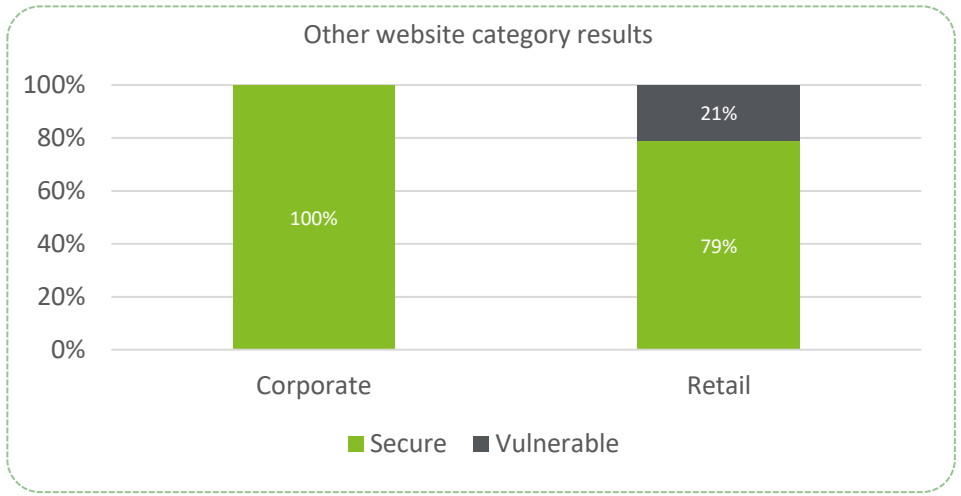
Websites using one of the few common 1024-bit Diffie-Hellman groups can be susceptible to passive interception by attackers with the appropriate resources. To increase the reliability of key exchange, you should use larger prime numbers, such as 2048-bit prime numbers. It would be safer to switch to a Diffie-Hellman protocol that uses elliptic curves. Elliptic curves do not suffer from common precomputation problems, which means that attacks on parameters that are barely computable can compromise only one connection and not all using a given group.

Weak retail category settings suggest that setting up security is not a priority. However, keep in mind that users often use the same login credentials, which means that if an attacker intercepts data from one website, it could access data on a more secure website.

This year’s assessment shows that 100% of the main bank domains tested were secure. No change is recorded from the previous year’s review.

100% of Business category domains tested were secure, while the percentage for the Retail category is 79%.





4. Traffic security

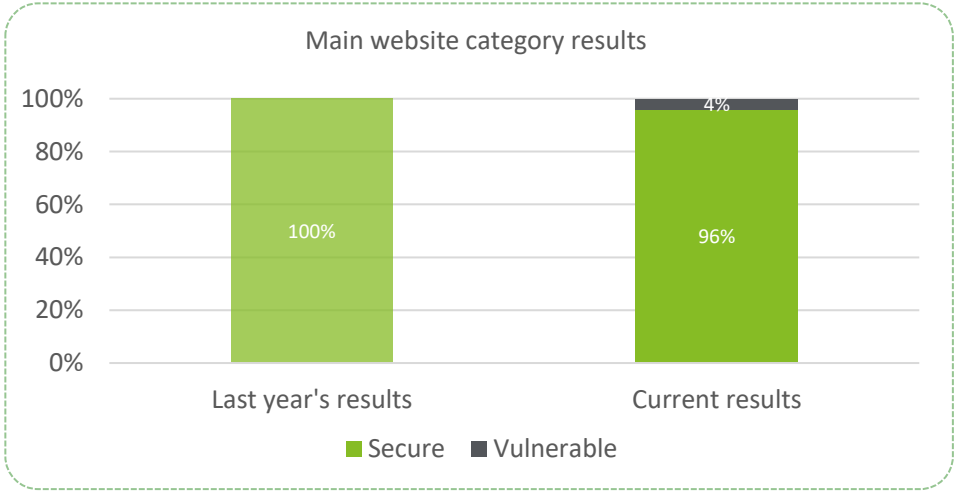
4.3 RC4 Support

RC4, also known as ARC4 or ARCFOUR, is a stream cipher widely used in computer networks (in SSL and TLS protocols, WEP and WPA wireless security algorithms) and various information security systems. The algorithm RC4, like any stream cipher, is based on a pseudo-random bit generator. The key is written to the generator input, and pseudo-random bits are read at the output. The length of the key can be between 40 and 2048 bits.

RC4 is no longer considered secure, and its feasibility requires careful consideration. For example, website RC4 support allows decryption of some encrypted HTTPS traffic (e.g., session ID passed to cookies) over tens of hours. It also becomes possible to implement a man-in-the-middle attack, eavesdropping and encrypted traffic storage, and the execution of a large number of requests on behalf of the victim.

The results for Business and Retail category domains tested were identical with 100% secure configuration.

As a result of the assessment, we concluded that the percentage of banks with "secure" results has dropped by 4% compared to the previous year.



100% of additional category websites do not use the RC4 algorithm

4. Traffic security

4.4 SSL 2.0 and SSL 3.0 support

SSL and TSL are encryption and authorization protocols that transmit data securely from server to server or from server to client. TSL is an improved version of SSL. However, some public web resources still support SSL for encryption.

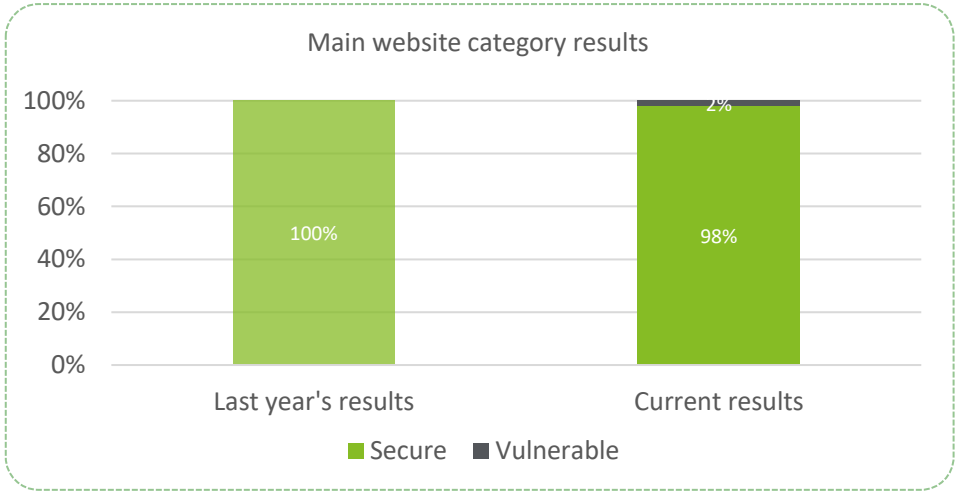
In 1995, SSL was first published by Netscape as SSL 2.0. This version, however, had a serious weakness, leading to its replacement in 1996 with a newer version, SSL 3.0.

Several vulnerabilities have been found in SSL 2.0 and 3.0 since the 90s, some of which were confirmed by IEFT in 2011 and 2015. Many of these vulnerabilities are no longer a threat, but in practice, SSL is not as secure as it should be.

Internet browsers that needed to combat security vulnerabilities, began warning users by flagging websites that used SSL certificates as insecure. These flaws give TLS many advantages. To switch to TLS, SSL 2.0 and SSL 3.0 must be disabled in server settings.

The assessment concludes that the percentage of good results has dropped by 2% compared to the previous year.

The results for the Business and Retail domain categories tested are identical with 100% secure configuration.



100% of websites of additional categories do not support the SSL

4. Traffic security

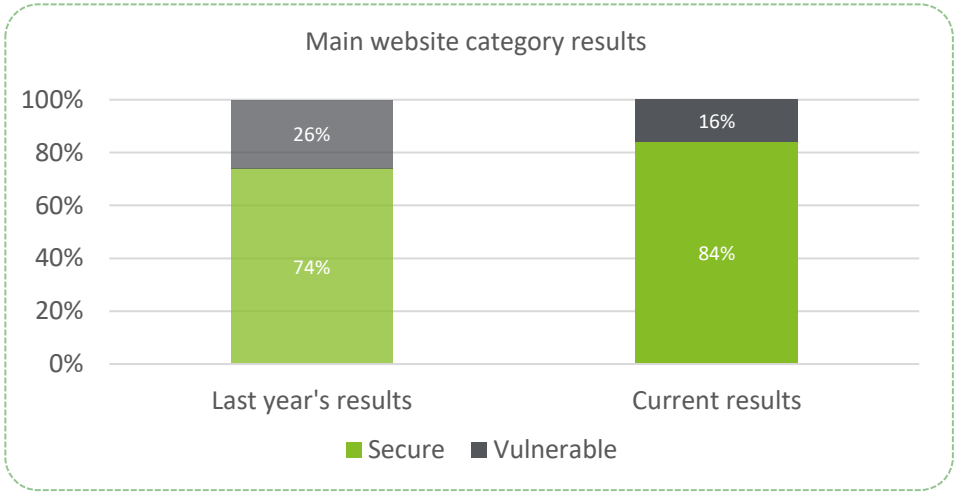
4.5 Outdated TLS versions

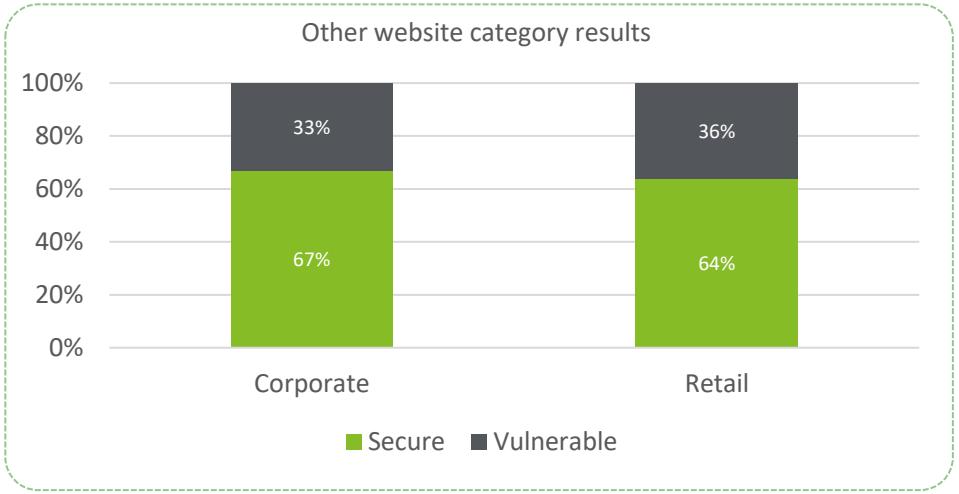
Transport Layer Security guarantees encrypted communication to ensure security and privacy. TLS version 1.0 has been around since 1999 and is an evolution of the older SSL encryption protocol. A more modern TLS 1.2 version appeared in August 2008, and the most current TLS 1.3 was released in August 2018.

In 2011, a vulnerability was discovered in TLS 1.0 that allows user authentication cookies to be decrypted. In addition, TLS 1.0 and 1.1 use unreliable MD5 and SHA-1 hashing algorithms. In 2020, all major browsers have disabled support for TLS 1.0 and TLS 1.1. Disabling these protocols is also recommended on the server side.

The research shows that 84% of main category domains have turned off support for legacy versions of the protocol, while corporate and retail category domains have turned off support in 67% and 60% of websites, respectively. A comparison with the previous year's survey shows a marked 10% improvement in the main domain category.

We recommend disabling website support for outdated versions, as their presence increases the potential threat of data decryption.





4. Traffic security

4.6 Beast Vulnerability

Attackers can decrypt data transmitted between two participants using TLS 1.0, SSL 3.0, and lower. The attacker and victim must be in the same network (man-in-the-middle) for the attack to work.

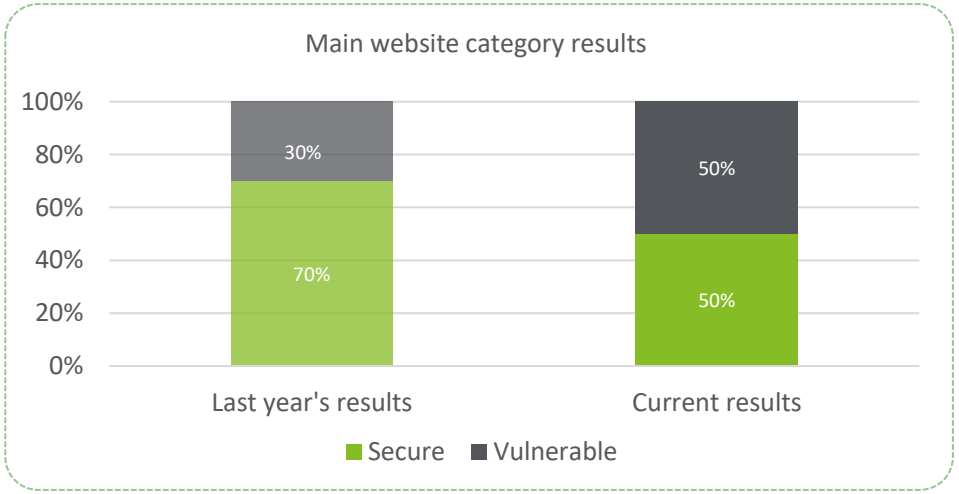
Using the BEAST method, passwords can be broken down into small packets and decrypted. Hackers who decrypt one byte of data in two seconds can gain access to credentials in half an hour using a 1000-2000 character authentication system.

The most effective way to protect users from BEAST attacks is to disable support for SSL and TLS above version 1.2 on the server side.

The research found that despite support for legacy SSL and TLS versions older than 1.2, the majority of retail websites mitigated the BEAST vulnerability on the server side. However, in the case of mainstream and corporate websites, the closeness of BEAST vulnerability percentages and support for legacy protocols suggests no mitigation of this vulnerability.

This year’s assessment shows that "corporate" and "retail" category domains were 100% secure, while the results for the "main" domains are 20% down, compared to the previous year.

We recommend that the remaining websites disable support for legacy versions of TLS or mitigate the Beast vulnerability, as support for older versions of TLS increases the risks of potential data interception.



100% of additional category websites
are assessed as secure

4. Traffic security

4.7 SSL Renegotiation

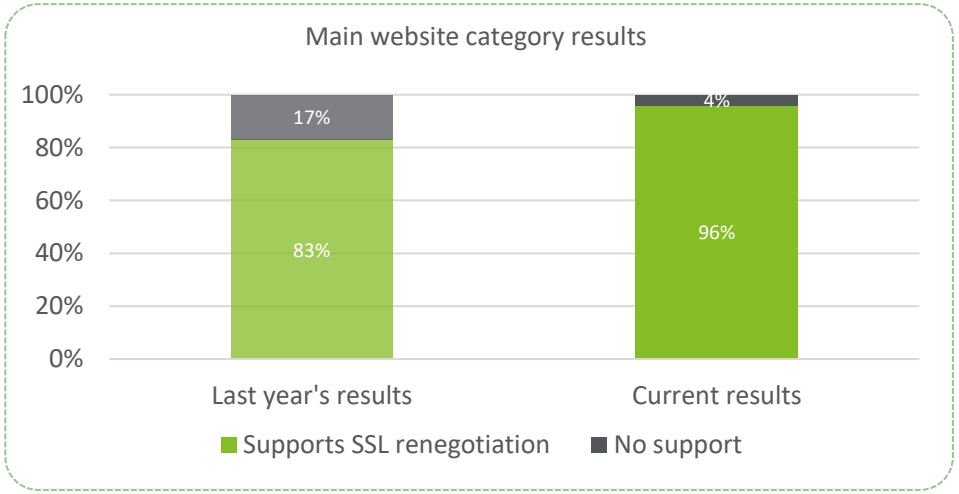
SSL Renegotiation - resuming reconnection to a server with existing authentication credentials within an existing secure session.

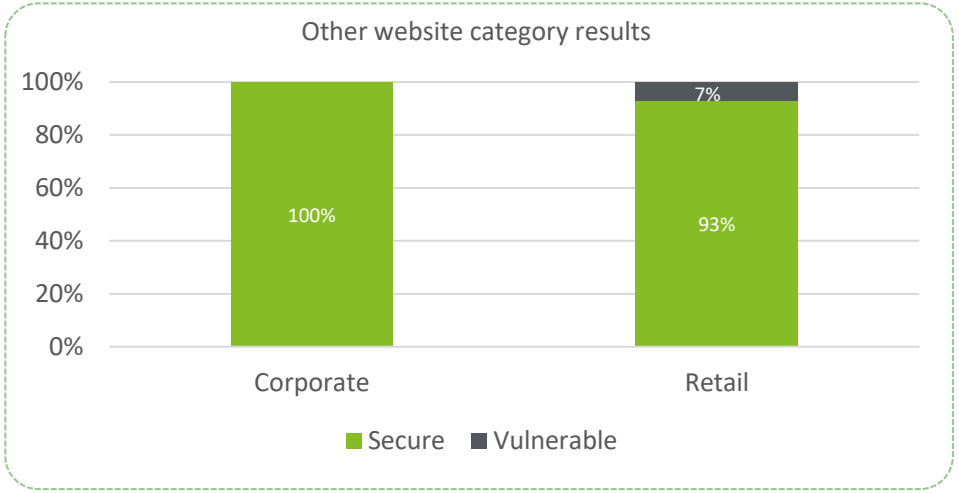
Misconfiguration of SSL Renegotiation can cause attacks such as Denial of Service (DOS) or Man-in-the-Middle (MITM) injection attacks in an HTTPS session. Therefore, some developers prefer to disable server-side SSL Renegotiation.

However, disabling Renegotiation and not indicating security status cause problems as some servers will be secure, others will not, and browsers can do nothing without having information about server reliability. This makes users uncomfortable and forces them to manually configure security levels.

The study shows that 100% of the "corporate" category and 93% of the "retail" category have set up SSL Renegotiation. The performance of the "main" category has improved significantly since the previous year's survey, increasing support for secure connection renegotiation by 13%.

We recommend configuring the server to allow only secure SSL Renegotiation and limit the number of SSL connections.





4. Traffic security

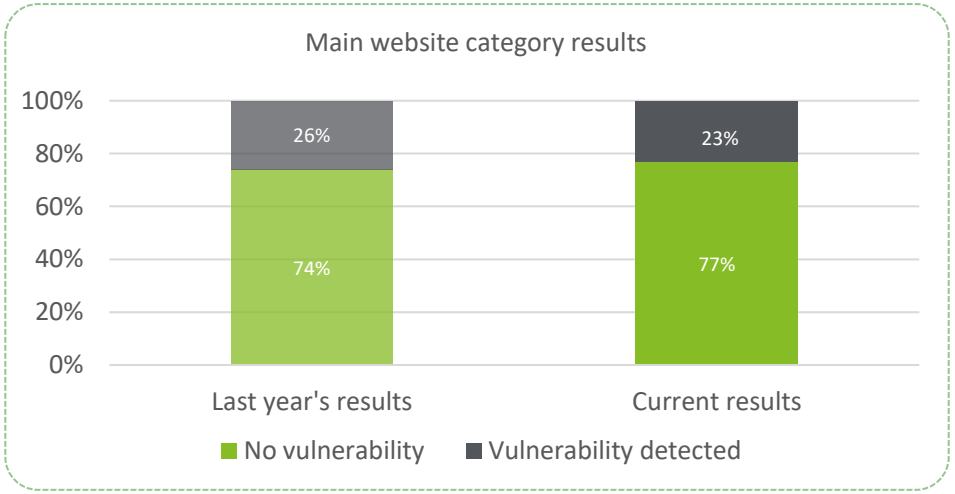
4.8 Ticketbleed SSl vulnerability

At the beginning of 2017, a vulnerability appeared that only affects F5 products. Ticketbleed is software vulnerability that allows an attacker to remotely fetch up to 31 bytes of uninitialized memory simultaneously on a stack of F5 BIG-IP TLS/SSL devices. This memory can store potentially sensitive information or sensitive credentials from other connections.

The study shows that 77% of "main" category websites have no Ticketbleed vulnerability. Compared to the previous year's survey, the results show a 3% point improvement.

"Corporate" and "retail" category websites show no Ticketbleed vulnerability.

Websites vulnerable to Ticketbleed should update their TMOS version to strengthen domain protection.



100% of additional category websites show no Ticketbleed vulnerability.

4. Traffic security

4.9 Other SSL vulnerabilities

In addition to the above observations, we checked each target in the scope of this Report for ROBOT, POODLE, GOLDENDOODLE, FREAK, DROWN and Heartbleed vulnerabilities.

We found that none of the local bank websites were exposed to any such attacks.

100% of websites
have no vulnerability to these attacks

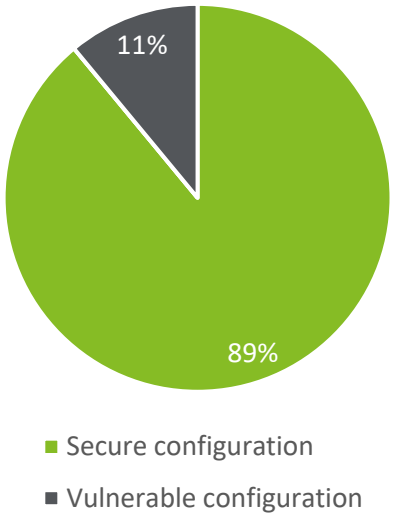
4. Traffic security

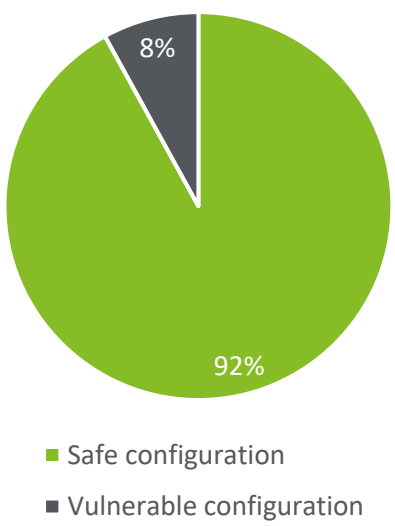
Conclusions

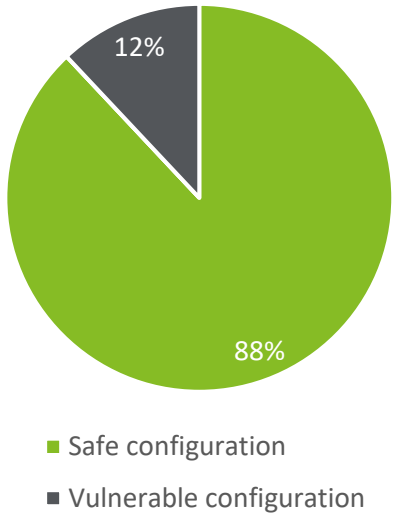
Implementing TLS is essential to ensure the security of online data both for banks and customers. However, improperly configured web servers can expose data rather than protect it.

A summarized assessment showed that 89% of bank sites in Azerbaijan have set up SSL/TLS configurations properly. However, some banks still maintain outdated versions of the protocols, making them vulnerable to potential attacks.

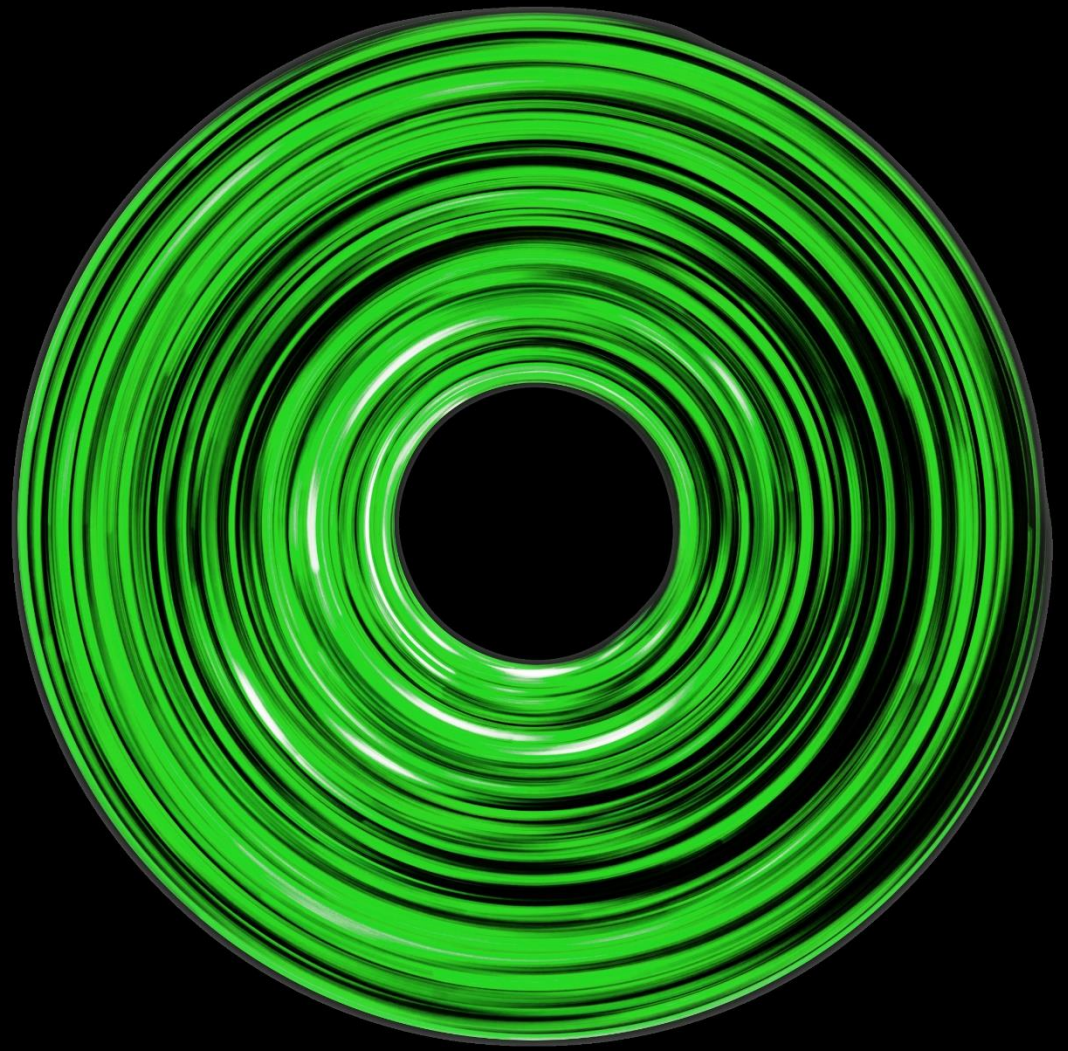
The summarized results for all traffic protection categories by country:







5. Mail server security



5. Mail server security

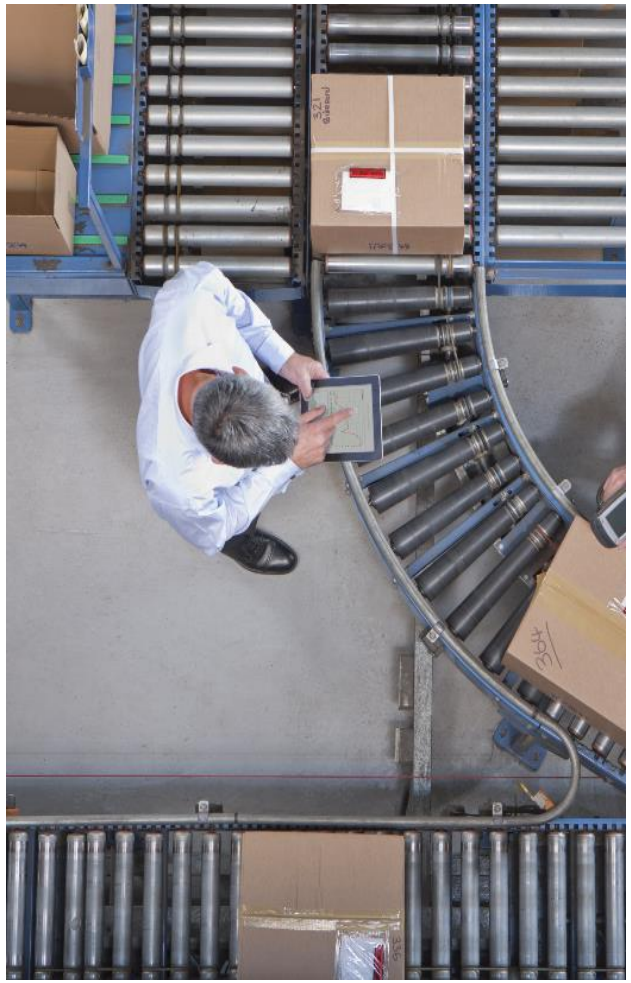
A common entry point for attackers seeking to gain a foothold in a corporate network and gain valuable banking data is email. The main problem with email is its insecurity. Vulnerabilities associated with email allow attackers to cause inconvenience and various problems compromising companies whether it be spam, malware, phishing attacks, sophisticated targeted attacks, or corporate email address leaks to the public. As most organizations use email to conduct business, email is often one of the top attack vectors for hackers.

Before applying complex protection methods, it is important to make sure that basic security settings are applied to protect company employees and improve overall email reputation. Very often spam filters will ignore emails sent from the bank's server, not perceiving them as malicious.

A list of mail (MX) servers with the server name of each bank (using MX Lookup) was compiled to analyze basic mail server security settings. The following security settings were then checked using the SMTP diagnostic tool from mxtoolbox.com:

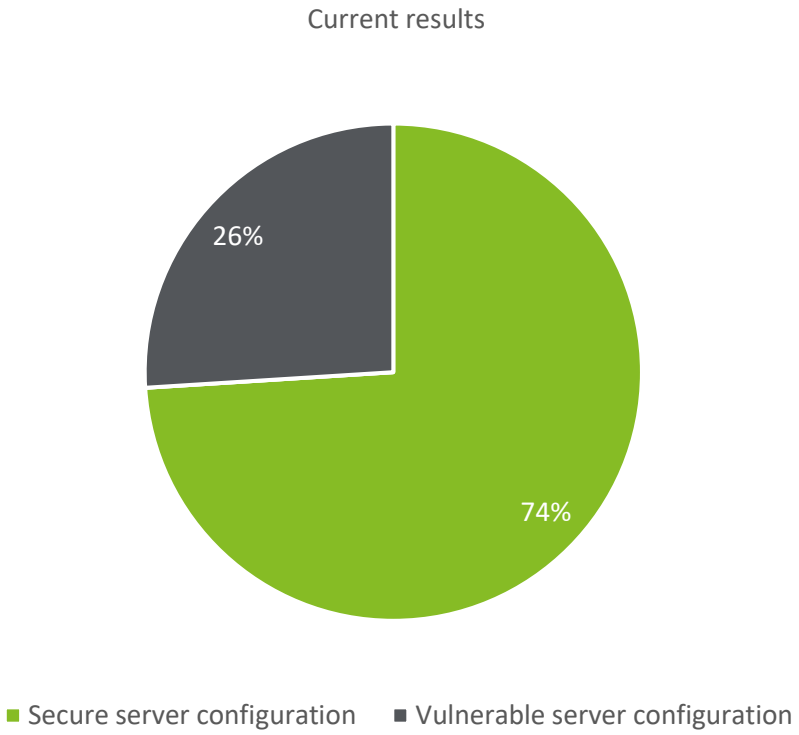
- SMTP Valid Hostname
- SMTP Banner
- SMTP TLS
- SMTP Open Relay
- SMTP Connection Time
- Domain Keys Identifies
- DMARC
- Mail

A TLS certificate validity check was also carried out using checktls.com.



5. Mail server security

Summarized security results of the "main" category mail servers



Analysis of the results shows that banks have a good score, but a small percentage still do not pay attention to the correct configuration of their mail servers.

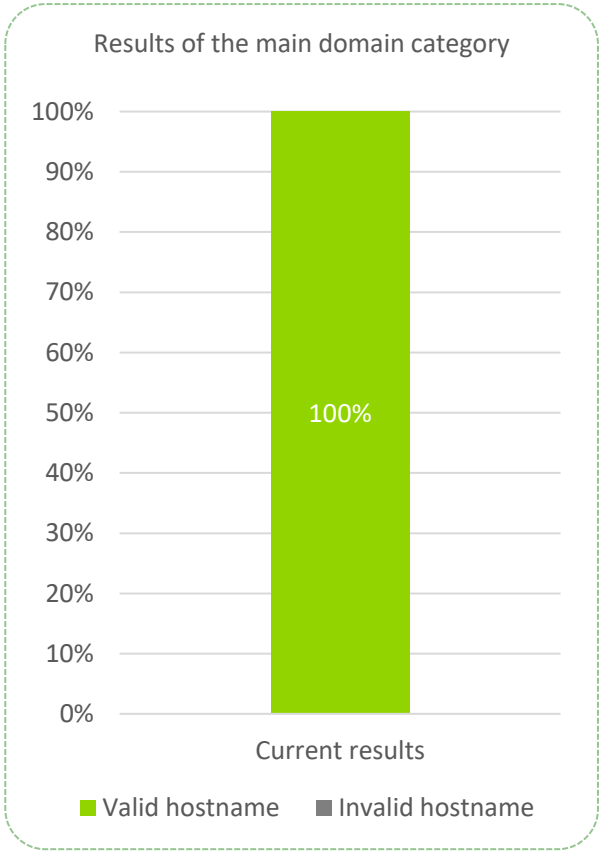
5. Mail server security

5.1 SMTP Valid Hostname

The test checks whether the "Reverse DNS Record" (PTR) is a valid hostname. According to best practices for sending emails, the PTR record must be a valid hostname. If the PTR record is not a valid hostname, there may be spam protection service problems when an email is delivered.

MxToolbox provides two assessments of hostname correctness: a valid hostname or an invalid hostname.

The assessment showed that 100% of the main bank domains have valid SMTP hostnames.



5. Mail server security

5.2 SMTP Banner Check

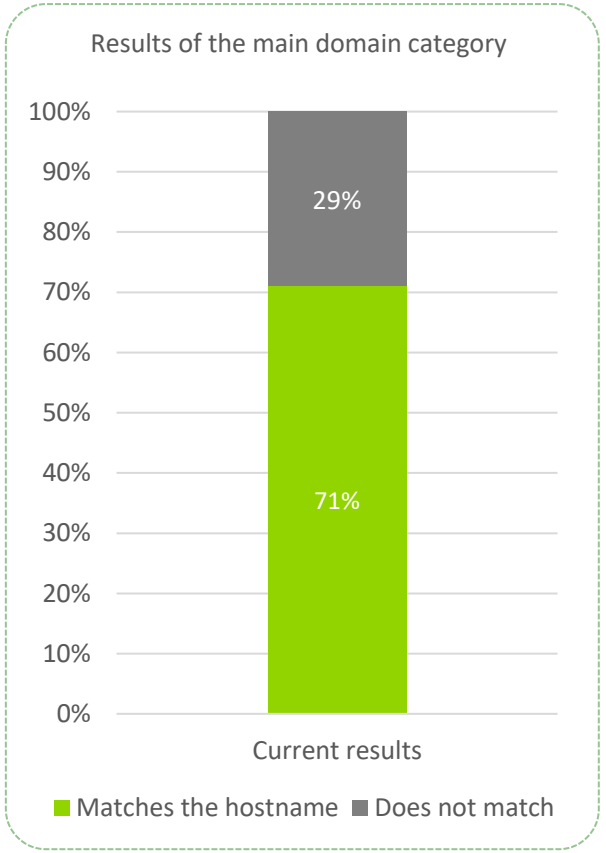
E-mail servers respond to connections on port 25 with a string of text called the SMTP banner, whose main purpose is to announce the server and any information that the administrator would like to provide to the party establishing the connection. It is best to include the server name in the SMTP banner so that anyone who connects to the IP address will have an idea of whom they are "communicating".

Until recently, many servers "masked" their SMTP banners by replacing the characters with asterisks for anyone outside the local network. The underlying logic behind this was that the owners did not want to disclose any information about themselves for fear of providing information that might aid a possible attack on the server. The benefits of this are minimal, and many servers do banner checking as part of their anti-spam protection, so this practice has its downsides.

Some mail servers may use an inappropriate or masked banner as an indicator of a possible spam source in the scoring system, but most will not reject incoming mail solely on that basis.

According to the results, 71% of hostnames match the reverse record (PTR).

We recommend organizing/updating the reverse (PTR) record, which will match your mail server hostname.



5. Mail server security

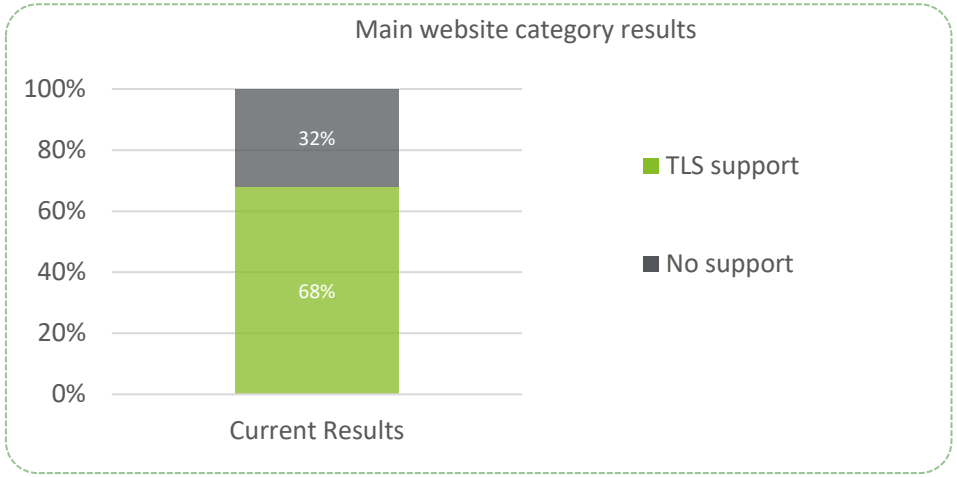
5.3 SMTP TLS

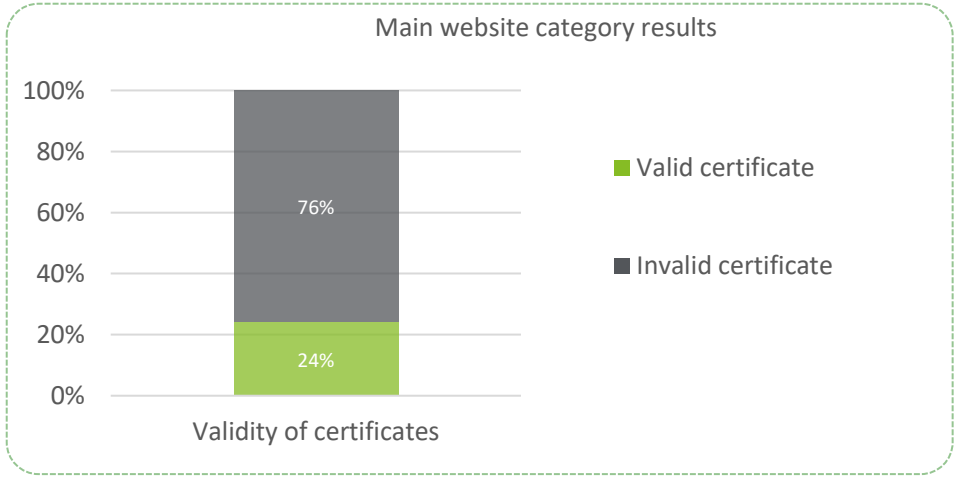
TLS stands for Transport Layer Security and allows mail servers to exchange emails over an encrypted connection using the same mechanism as HTTPS to protect web traffic. In all but a few cases, you will still be able to send and receive an email, but your messages will be transmitted as plain text without TLS encryption.

According to the result, 68% of mail servers support TLS. In 32% of cases, mail servers failed when trying to establish a secure SMTP connection.

In addition to TLS support, the study also tested the validity of certificates. It was determined that 68% of mail servers support TLS, however, only 24% successfully passed the certificate validity check.

We recommend combining TLS-based email encryption with email authentication to ensure the integrity of email messages.





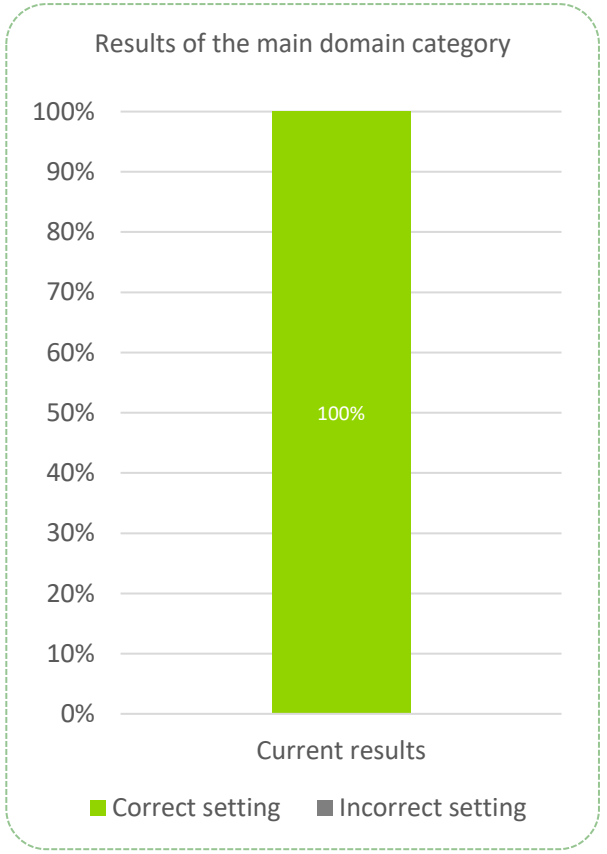
5. Mail server security

5.4 SMTP Open Relay

Many mail servers now pretend to accept a misdirected email, but then discard the message without forwarding a response to the sender. This method is used to prevent information-gathering attacks. In this type of attack, an attacker tries to send thousands of auto-generated emails from your server in an attempt to find valid email addresses. If your server responds with an error (5xx), the attacker will know that it is not a real email address. If your server accepts the message (2xx), the attacker will know that the address is valid.

During the study, messages were simulated to be sent to a deliberately wrong e-mail address (test@example.kz). Then, based on the responses received, it was determined whether the server is an open relay, i.e. whether it receives mail from an unknown server and then passes it to the corresponding server.

According to the assessment results, 100% of the banks received a "correct setting" rating.



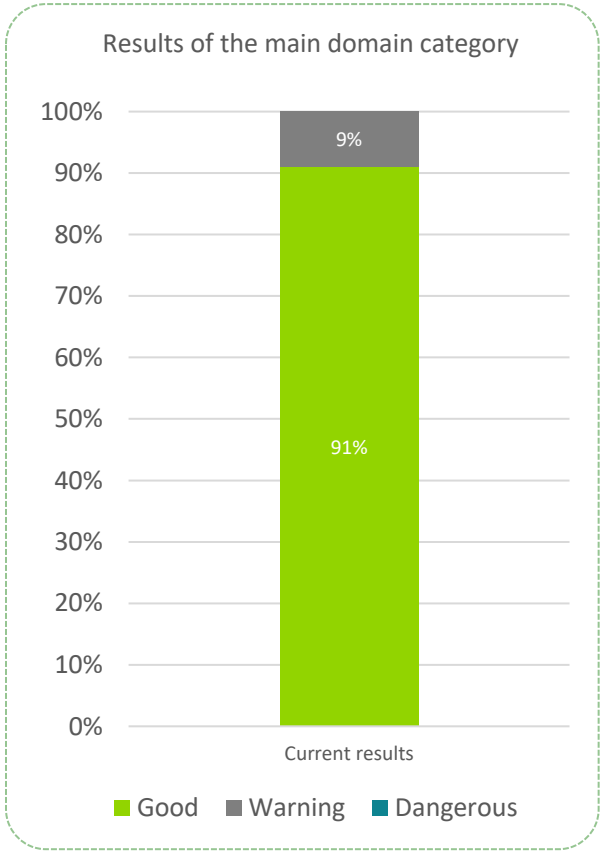
5. Mail server security

5.5 SMTP Connection Time

While checking SMTP Connection Time, the device connects to the mail server through open ports and sometimes it takes much longer to connect than expected. This may indicate that the mail server is under heavy load.

The response result to the connection time check request is measured in seconds. A response time of less than 5 seconds is considered a fast response time and falls into the "Good" category, a response from 5 to 8 seconds is a "Warning", and above 8 seconds is "Dangerous".

No mail servers were rated "Dangerous" as a result of the study, but 9% of mail servers responded within 5 to 8 seconds. This does not mean that there will be problems with mail forwarding, but for now, it is just a warning that the situation is not perfect. If mail volume increases or data bandwidth is reduced, this could lead to delays in mail forwarding.



5. Mail server security

5.6 DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) technology is used to prevent "spoofing" when sending emails from your domain.

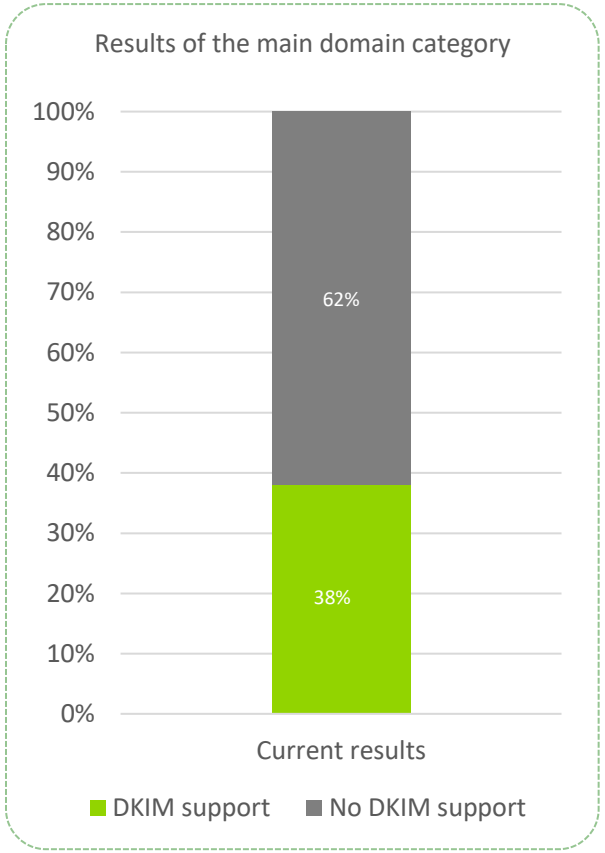
Spoofing is the modification of an email by an attacker that allows it to impersonate another person. To prevent spoofing, some email servers require that you authenticate the sender with a DKIM key.

DKIM technology allows an encrypted signature to be added to the headers of all outgoing messages. Email servers decrypt the headers of incoming messages and check to see if the message has changed since being sent.

DKIM signatures increase email security and help to prevent spoofing.

Review results determined that 38% of banks use their own DKIM key for all outgoing messages.

Since spoofing emails from trusted domains are becoming a more common cyber threat, it is important first to check your DKIM record to begin your DKIM implementation. We recommend that website owners add a DKIM record to their DNS whenever possible to authenticate email from their domain.



5. Mail server security

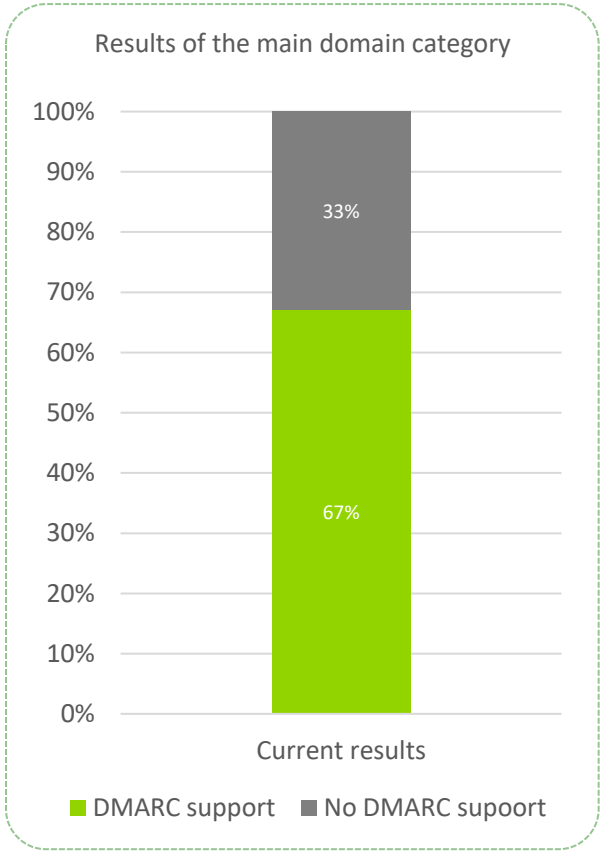
5.7 Domain-based Message Authentication Reporting and Conformance

Domain-based Message Authentication Reporting and Conformance (DMARC) is one of the mechanisms used to protect organizations from phishing attacks using their mail server. It is no secret that for a phishing attack to succeed, an email has to be as similar to a legitimate one as possible. The key to success in such a case will be the ability to send the email directly via the attacked organization's mail server.

In a secure implementation, the mail server checks whether the server email address in the "From:" line matches the SPF verification and DKIM signature identifiers. If there is an absolute match, the email is recognized as legitimate and sent to the recipient's mailbox. If there is the slightest mismatch, the message is processed according to the configured DMARC policy.

The result of the study showed that 67% of bank mail servers use this protection mechanism. In 33% of cases, it has not been applied yet.

We recommend that website owners add DMARC as it allows domain owners to protect their domains from unauthorized use by fighting phishing, spoofing, CEO fraud, and Business Email Compromise.



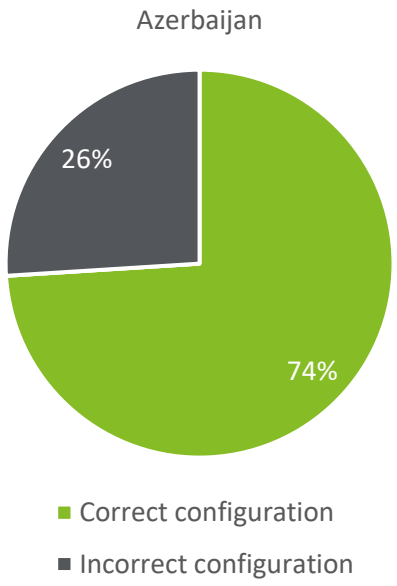
5. Mail server security

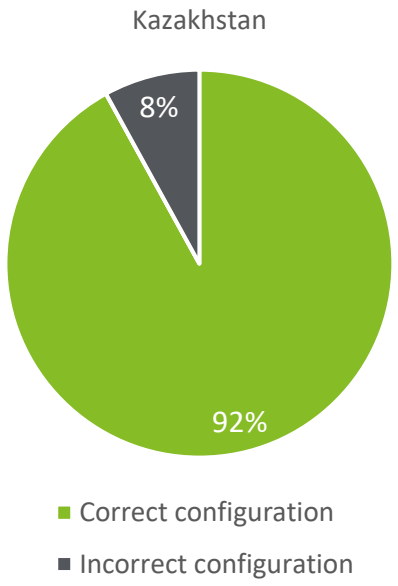
Conclusions

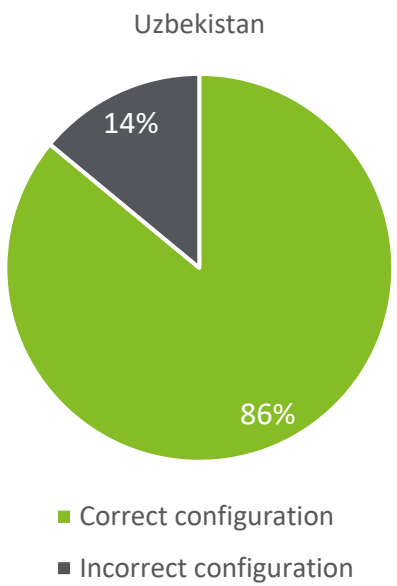
Despite the active use of all kinds of mobile messengers by bank employees, email remains an official communication tool. This applies both to interacting with internal banking structures and with external organizations. In this regard, ensuring a high level of security when working with email is an important task.

Results show that results are good. Nevertheless, banks in Azerbaijan have not yet applied some of the measures that increase protection levels. In this regard, we recommend vulnerable banks implement the necessary protection measures on mail servers.

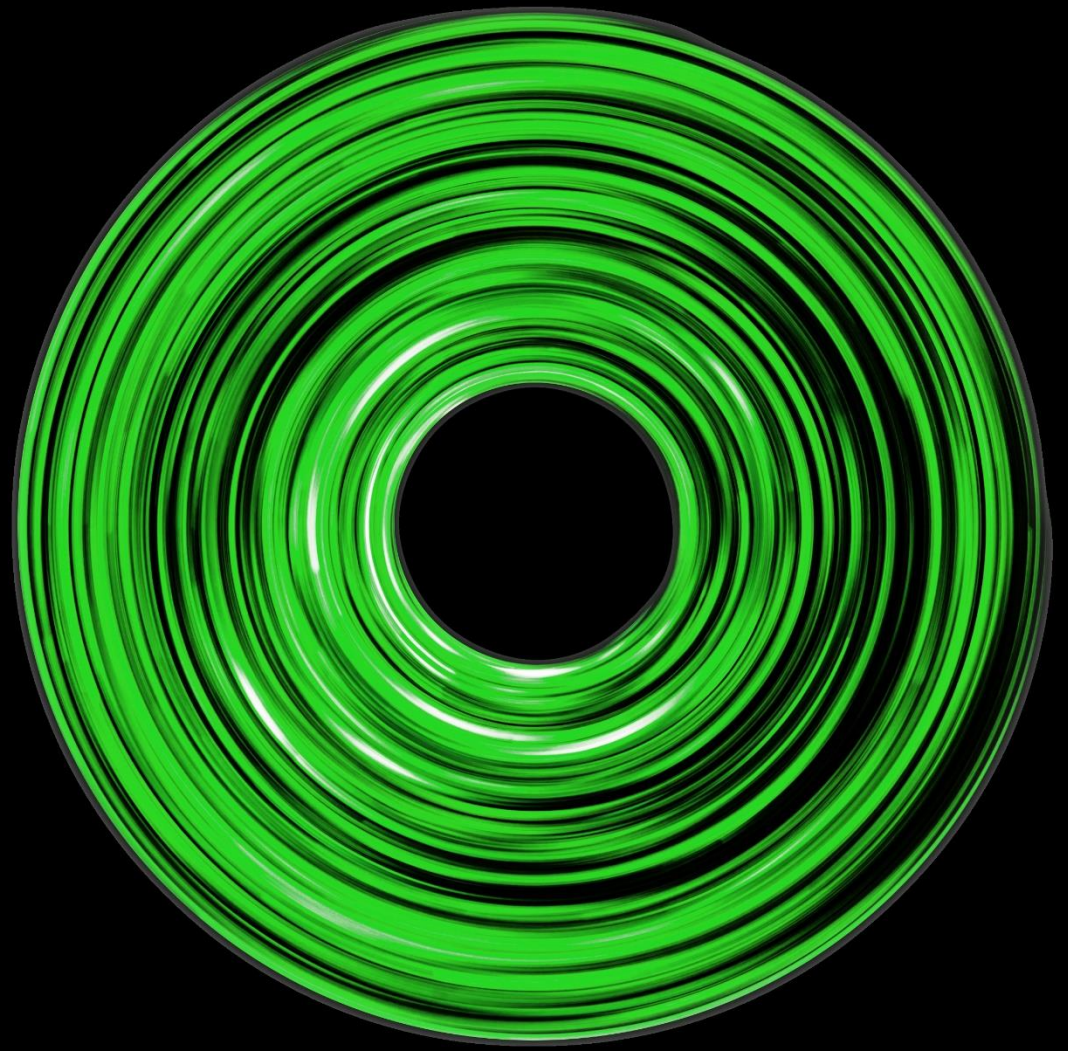
Summarized results for all categories of traffic protection, by country:







6. Email address leaks



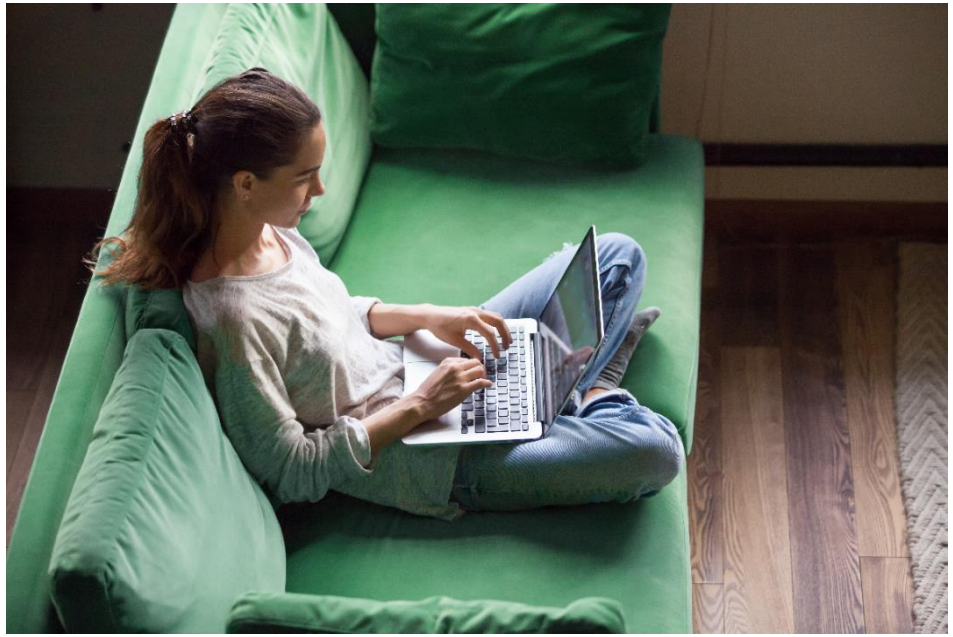
6. Email address leaks

Data leaks are common across the world and are one of the disadvantages of the digital world. Even in cases where an organization protects its information resources responsibly and applies the most advanced technical protection tools, the human factor is still one of the most significant vulnerabilities.

Employees of organizations with little cybersecurity awareness often use corporate email addresses to sign up for third-party web resources. In itself, a corporate email address leaked in this way can be used to send unsolicited emails (SPAM) but the situation is made worse by the fact that the employees often use the same passwords or just change only one or two characters in their passwords. As a result, cybercriminals can get their hands on both the corporate email address and the password to it.

Having access to corporate emails can, for example, gain access to confidential or personal client information. It can also be used to conduct phishing attacks on other employees of the organization. The specific consequences of these types of leak are difficult to predict, but will most likely be negative.

There are resources on the Internet that help organizations determine if any of their accounts has been compromised during a data breach. Anyone can use haveibeenpwned.com to find out if a particular email has been exposed to a leak, and if so, the service will provide detailed information about them.



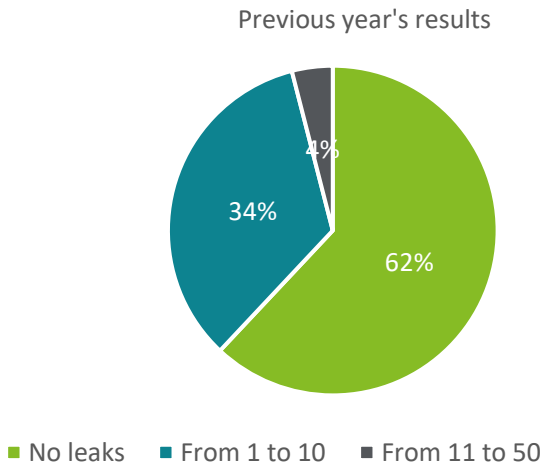
6. Email address leaks

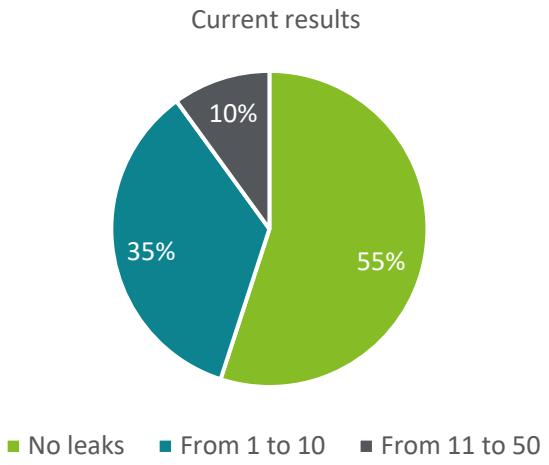
6.1 Our leak assessment approach and its results

We studied publicly available information from social networks (e.g., LinkedIn) for this Review and used it to form a target list of Azerbaijan bank employees. Next, using the Hunter.io Internet resource, we identified the email templates used by banks and generated a list of target email addresses for each bank. The lists of emails we generated were checked against those of leaked emails. The Internet service haveibeenpwned.com was used for this purpose.

The resulting statistics are summarized in the graphs on the right.

The results indicate that 45% of email leaks still occur. However, a comparison of the current figures with the previous year's is encouraging. As we can see from the statistics, the percentage of leaks and their scale has decreased. This is most likely the result of internal work done by banks to raise awareness among employees.





6. Email address leaks

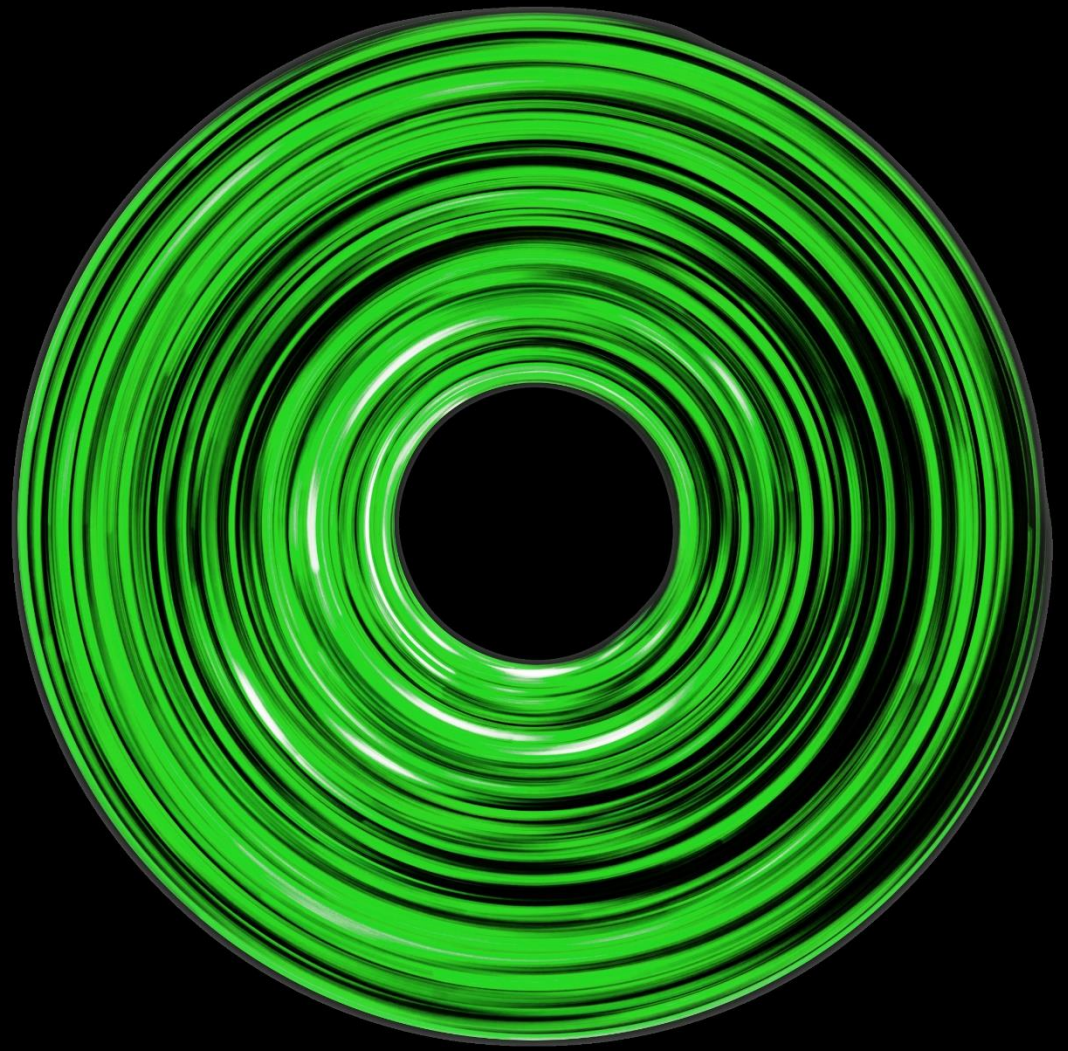
Conclusions

To reduce the risk of possible email address leaks, we recommend developing and maintaining a cybersecurity training program for employees, which can be based on:

- Conducting a phishing test to assess current levels of employee awareness and identifying risk areas;
- Preparing training materials for personnel in cybersecurity areas. Particular attention should be paid to those issues where major gaps were identified in the first phase. In addition to the training course, materials may include visual aids, stands and flyers, special informational videos to be used as screen savers, and informational pictures in the form of background images to be used on all computers in the organization;
- Conducting interactive seminars or online training with the presentation of prepared materials. At the end of the training, employees should be tested to assess the knowledge acquired.

Summary of email address leaks by country:

7. Compliance with personal data protection requirements

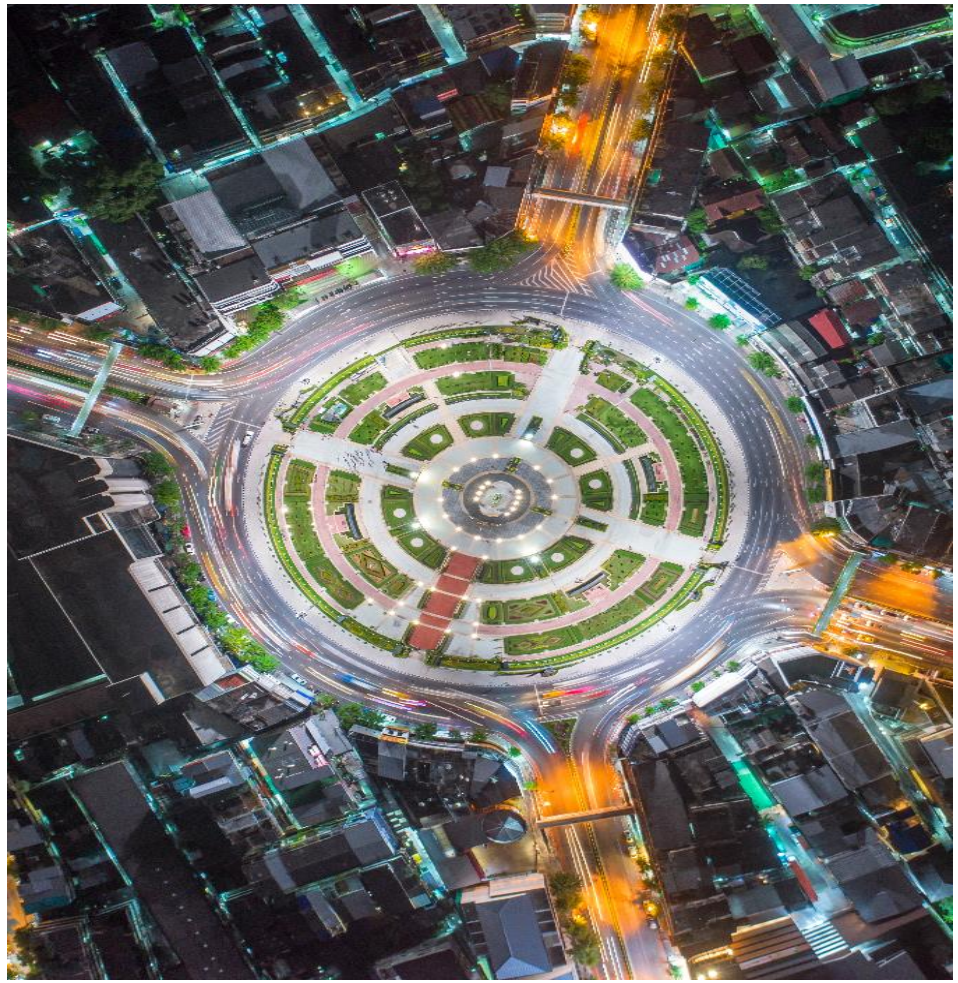


7. Compliance with personal data protection requirements

The GDPR, or General Data Protection Regulation, is an EU data protection and privacy regulation that applies to all persons in the European Union. It applies to any work and services that involve the collection and processing of personal data of people residing in the EU.

According to European Commission regulations, personal data includes any information about an individual, whether related to his or her private, professional, or public life, such as name, home address, photo, email addresses, banking information, social media messages, medical information, or IP address. This means that websites should not collect statistical data and personal information or store unnecessary COOKIE files for the technical operation of the site without prior consent from the user.

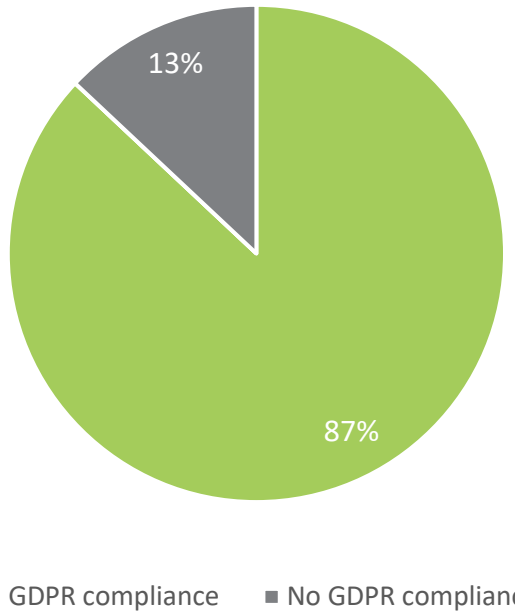
It should be noted that for the purposes of this Review, the absence of any collection of information through COOKIEs has been interpreted as GDPR compliance.



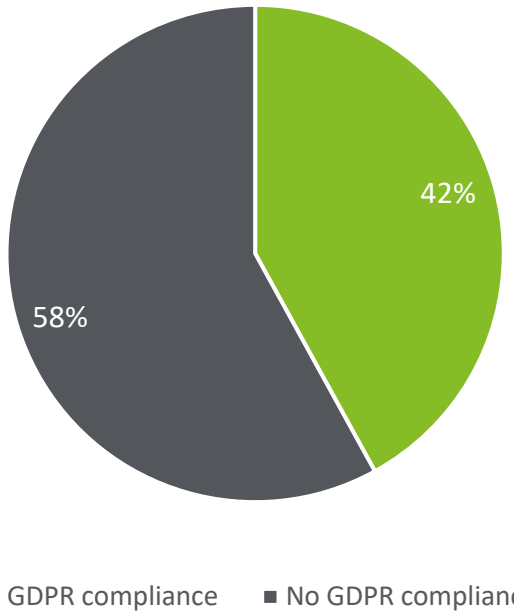
7. Compliance with personal data protection requirements

Summarized results for GDPR requirements of “Main" category websites

Previous year's results



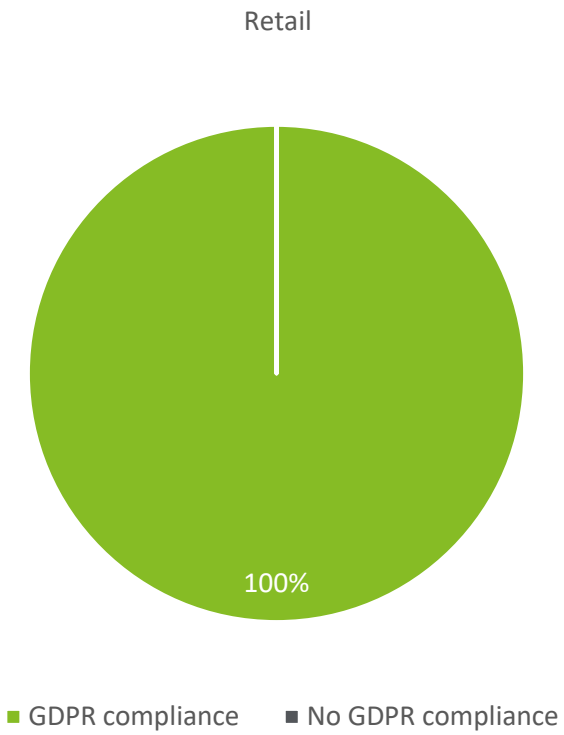
Current results

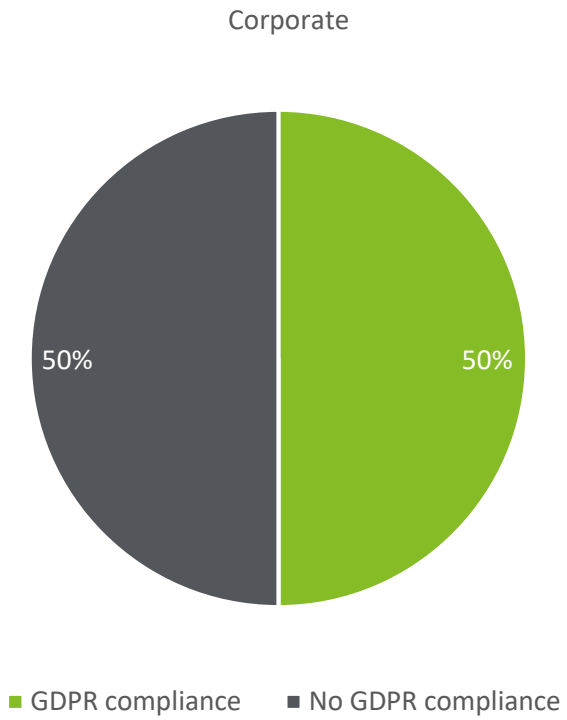


The current year's results show that the number of banks meeting this requirement has shrunk compared to the previous year.

7. Compliance with personal data protection requirements

Summarized results for GDPR requirements in the “Corporate" and “Retail" categories





Most Azerbaijan bank websites in the "Corporate" and "Retail" categories are GDPR compliant.

7. Compliance with personal data protection requirements

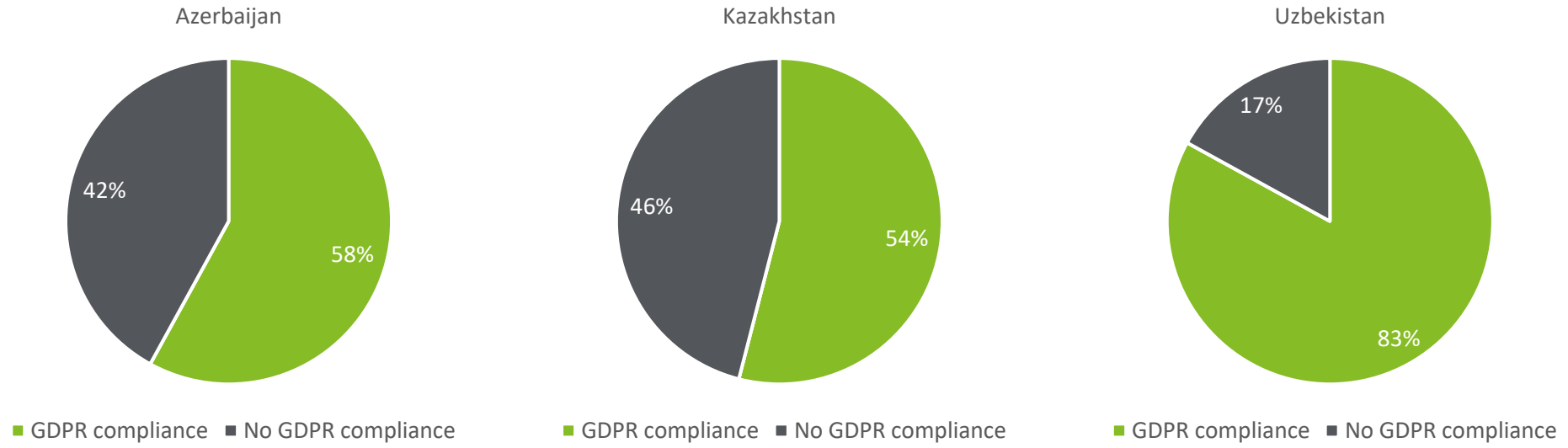
Conclusions

Azerbaijan law does not require companies providing financial services to comply with GDPR requirements.

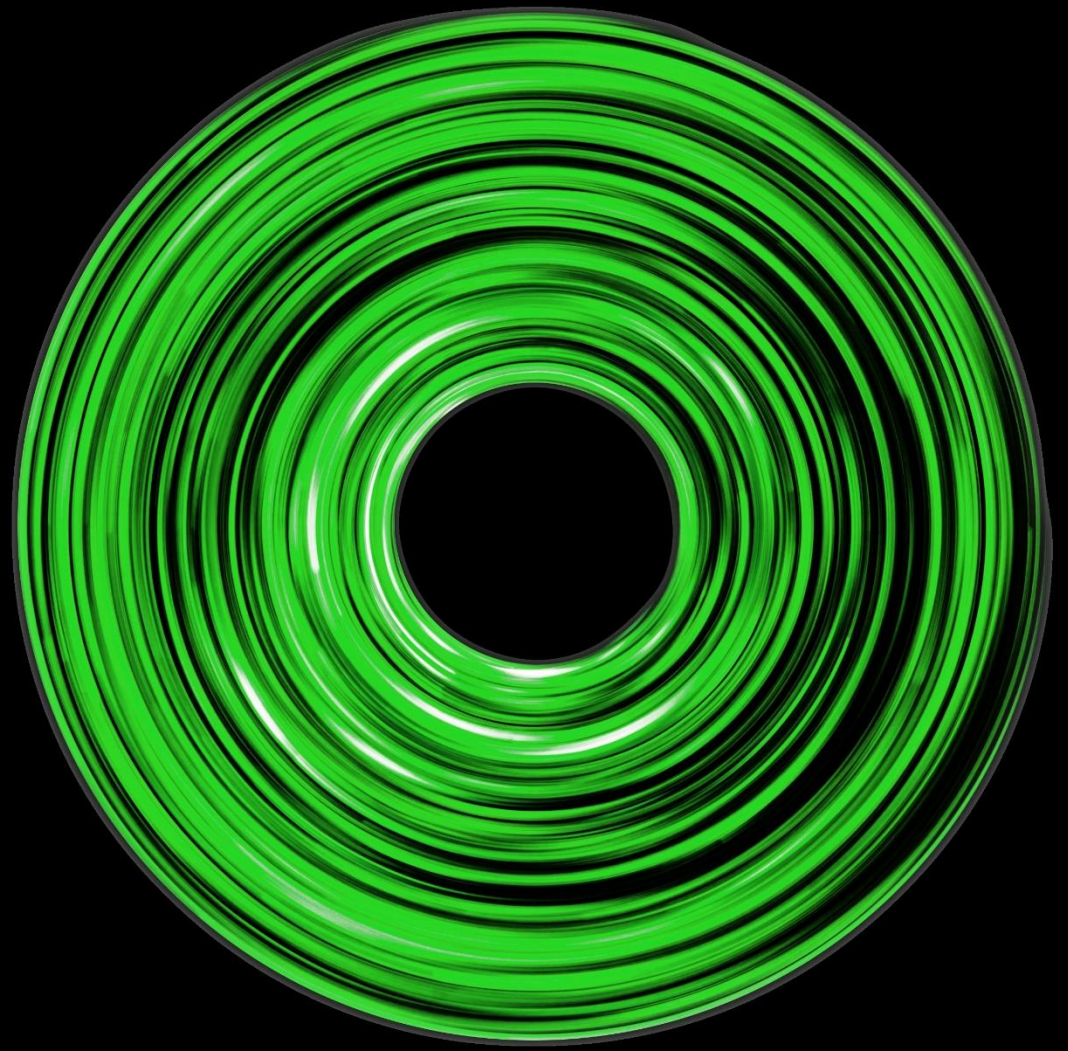
However, GDPR Article 3(2), which deals with territorial coverage, states that even companies established outside the EU are subject to GDPR requirements if they offer goods or services to individuals (data subjects) residing in the EU, or monitor the behavior of such persons, regardless of whether payment is required from the data subject. In other words, if any bank holds data of at least one customer who is a citizen of the European Union, it is automatically subject to GDPR.

Moreover, GDRP compliance can be a decisive factor for potential customers (especially if they are from the EU) looking for a financial services provider in Azerbaijan.

Summarized GDPR compliance results for all website categories, by country:



8. Open ports



8. Open ports

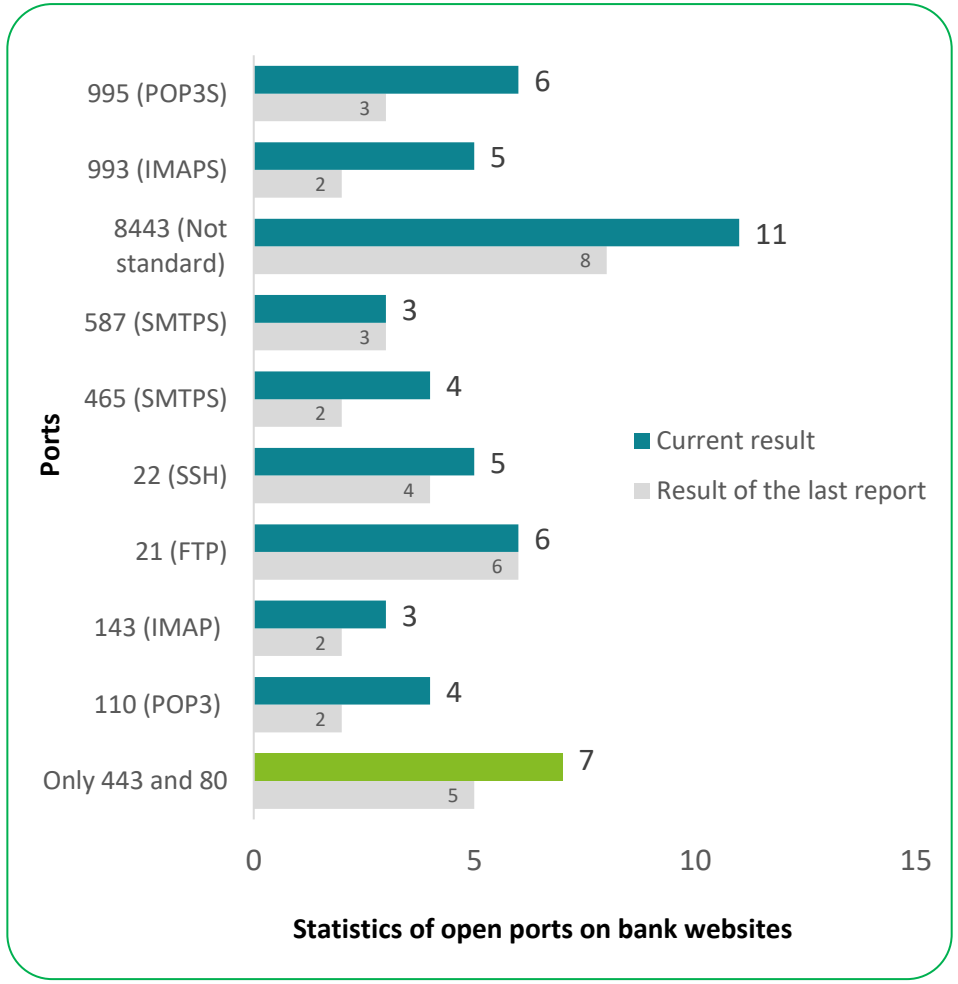
Best practices state that ports (services) that are not essential to the operation of a website should be closed or filtered.

As part of this Review, a list of open ports on bank websites was analyzed. The online scanning service nmap.online-domain-tools.com was used to determine the status of ports. The study was limited to 100 ports on which the most common online services are located.

The results of the analysis of open ports on bank websites indicate that only 28% adhere to the recommendation to use ports 80 and 443 exclusively. Also, compared to the previous year's results, the number of such banks has increased by 2.

The main share of additional services that banks use are email services:

- port 110 - (POP3) is the most common method of receiving e-mail.
- port 143 - (IMAP) is another service for handling e-mail.
- Port 465 - (SMTPS) is the same SMTP but with TLS/SSL encryption.
- Port 587 - (SMTP) is a port that is mostly used to send mail to end users. It also supports TLS.
- Port 993 - (IMAPS) is the same as IMAP but with TLS/SSL encryption.
- Port 995 - (POP3S) is the same as POP3 but with TLS/SSL encryption.



8. Open ports

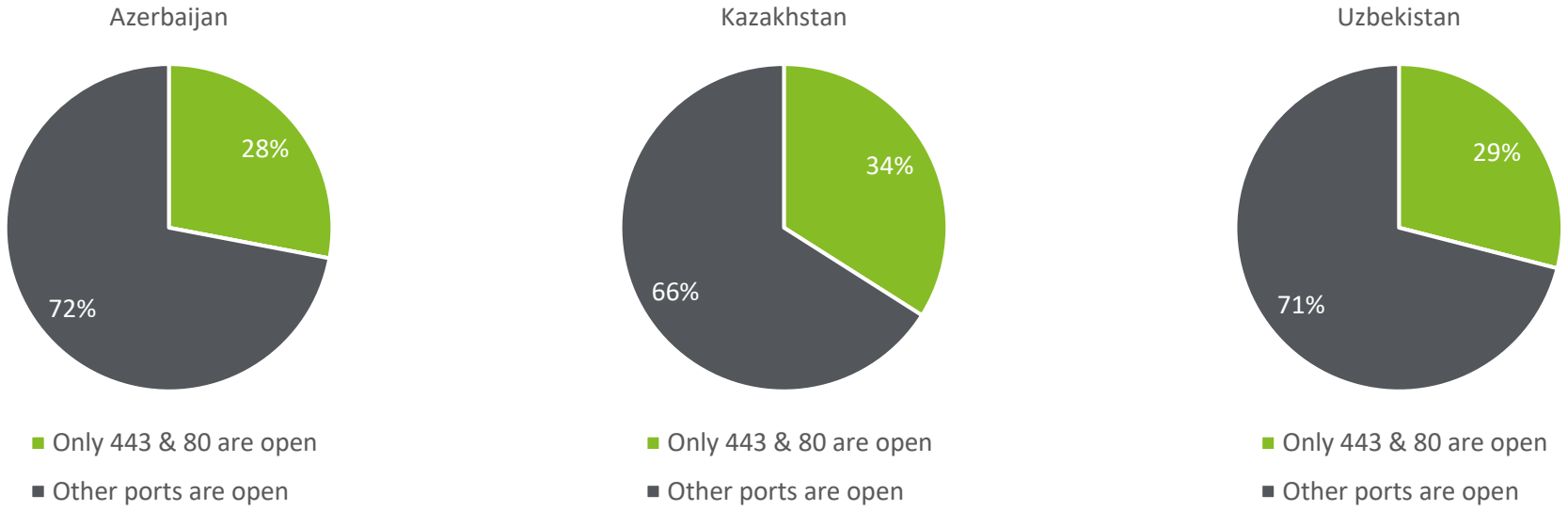
Conclusions

The summarized results on open port analysis indicates that in addition to the standard pair of ports 80 and 443, banks are actively using services such as e-mail, SSH, and even FTP on the same IP addresses.

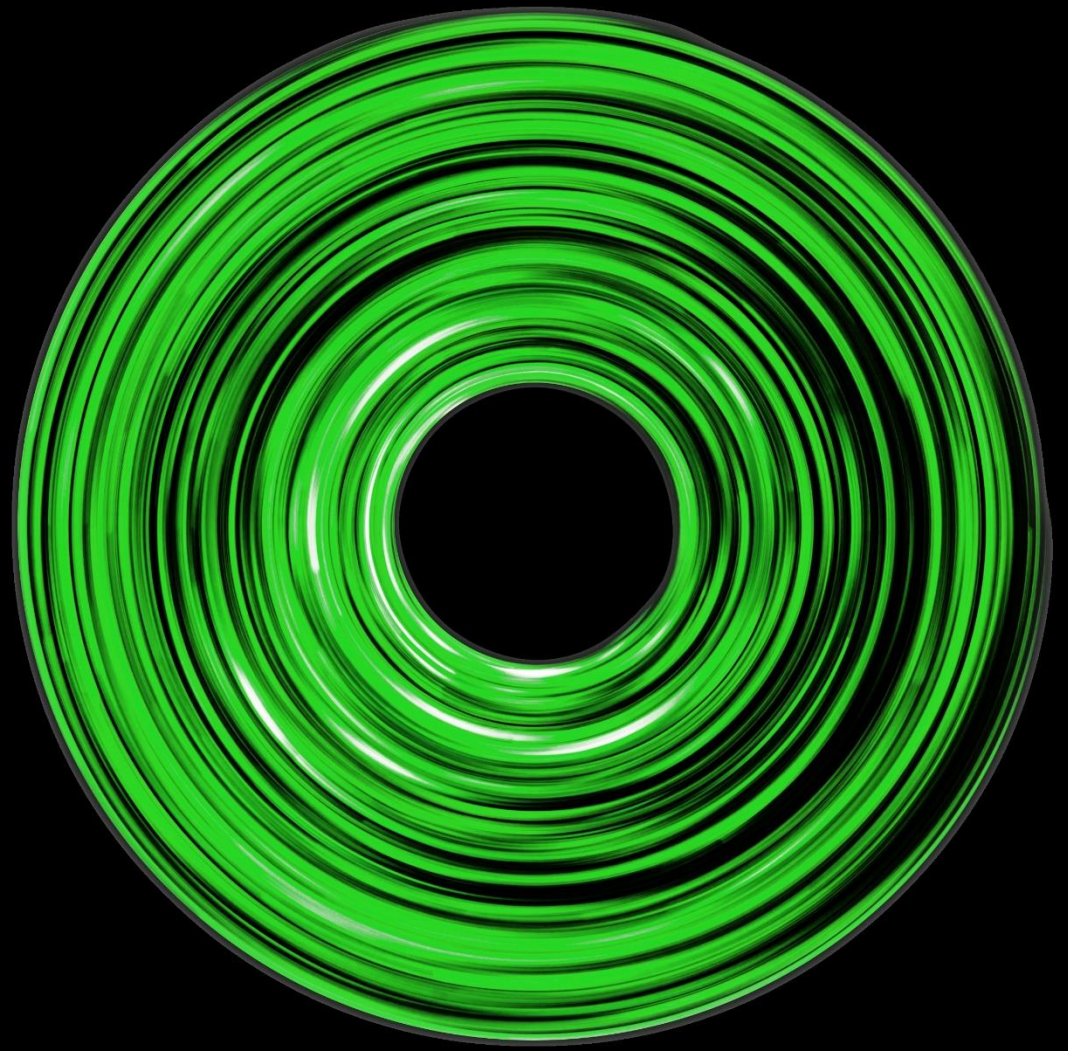
The analysis revealed the use of services on ports blocked by the majority of the world's Internet and cloud hosting providers, recommending the use of more secure equivalents. In this case, we are talking about switching to port 587. Port 2525 can also be used, even though it is not recognized as an official SMTP port, but is widely used and supported by most ISPs across the world.

Admittedly, this in itself does not pose any significant risks. Nevertheless, banks need to ensure that their processes for managing vulnerabilities, changes and IS incidents are working effectively.

Summarized results for open ports, by country:



9. Mobile banking security



9. Mobile banking security

Most banks offer their customers access to mobile financial services, which has increased the convenience and accessibility of banking services in Azerbaijan.

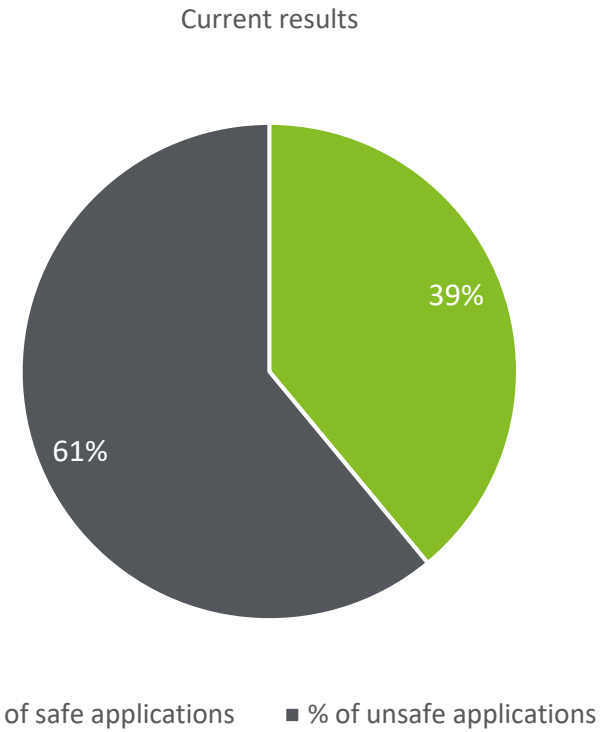
However, coupled with the unconditional benefits, the specificity and sufficient openness of mobile platforms make users of mobile devices a convenient target for attackers. In addition, a whole arsenal of hacker programs and tools has already been developed for mobile platforms, including viruses, trojans, fake banking programs, ransomware, and all kinds of spyware. This forces the developers of mobile banking applications, in addition to functionality and usability, to pay more attention to ensuring a high level of security.

Banking applications were tested to study the banking mobile applications on the two main platforms - Android and iOS. The following security parameters were examined as part of the study:

- Exposure to SSL Pinning attacks;
- Disclosure of confidential information in automatically generated screenshots;
- Checking safety protection mechanisms.

9. Mobile banking security

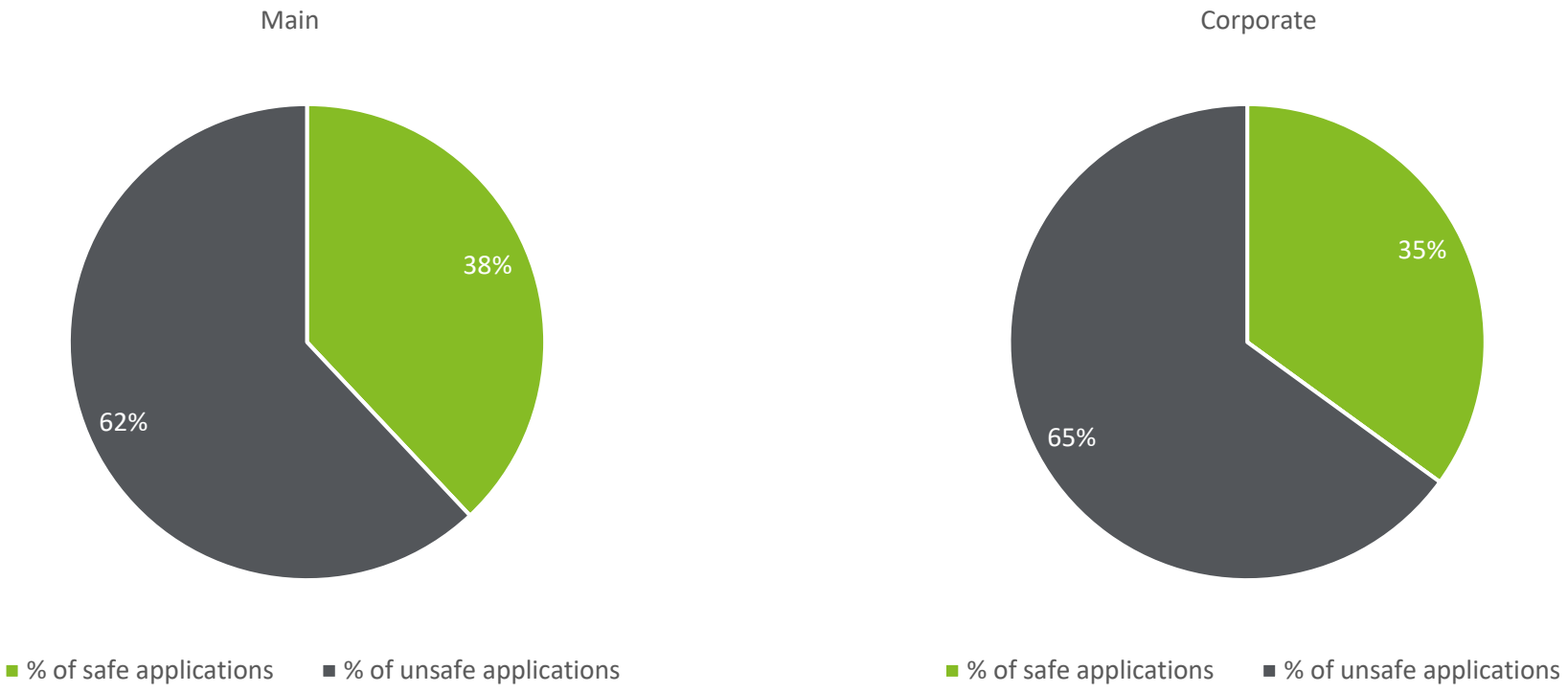
Summarized results on the Android platform



The research found that only 39% of banks follow secure mobile app development guidelines

9. Mobile banking security

Summarized results of both platforms for the "Main" and "Corporate" category



The research found that only 35% of "corporate“ category banks follow secure mobile app development guidelines

9. Mobile banking security

9.1 Exposure to SSL Pinning type attacks

SSL pinning is an attack on the cell phone owner in which the client's built-in SSL certificate matching mechanism is bypassed by simply installing "insecure" certificates.

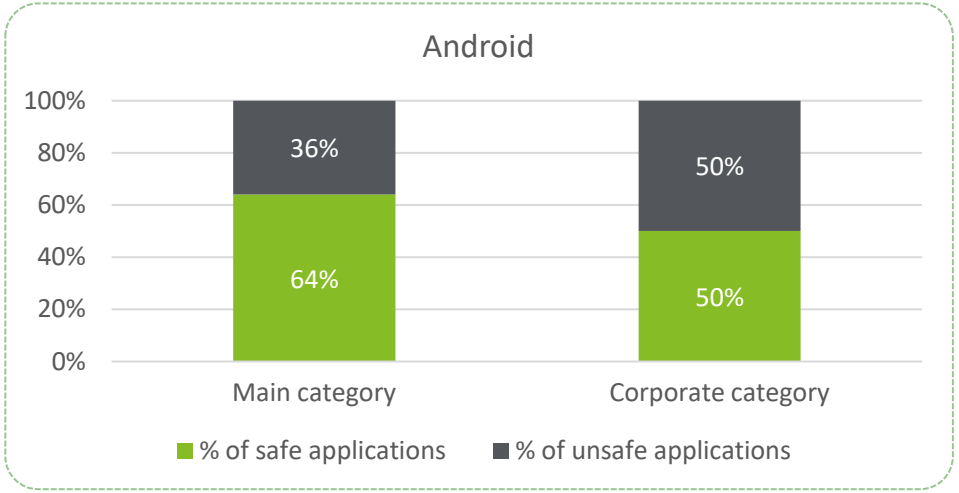
One simple way to protect against this threat is to embed an SSL certificate directly into the mobile app's code. In this case, the application will ignore the device's certificate storage and will use only the "hard-code" in the program certificates. As a result, this will allow secure data exchange with a web-based bank server.

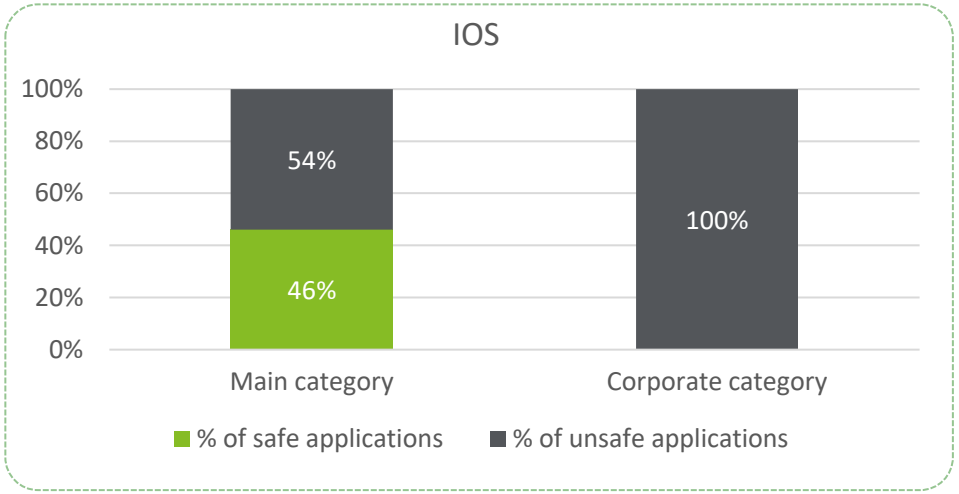
To verify SSL Pinning, a fake certificate was created and installed in smartphones for both platforms being tested. Traffic was then passed through a specially configured proxy server and intercepted for further analysis. Random login credentials were entered on the mobile devices, and then the intercepted traffic was analyzed for the credentials entered.

If the credentials entered in the mobile app were intercepted in transmitted traffic in clear form, the app was rated as unprotected. Conversely, if the transmitted data remained encrypted despite a fake certificate, the app was considered secure against SSL Pinning.

The SSL Pinning for Android devices showed that the current security result is 64% for the "main" category, and the result for "corporate" applications showed only 50% security.

As for SSL Pinning verification for IOS devices, the research showed that 54% and 100% of the "main" and "corporate" category apps are not secure, respectively.





9. Mobile banking security

9.2 Disclosure of confidential information in automatically generated screenshots

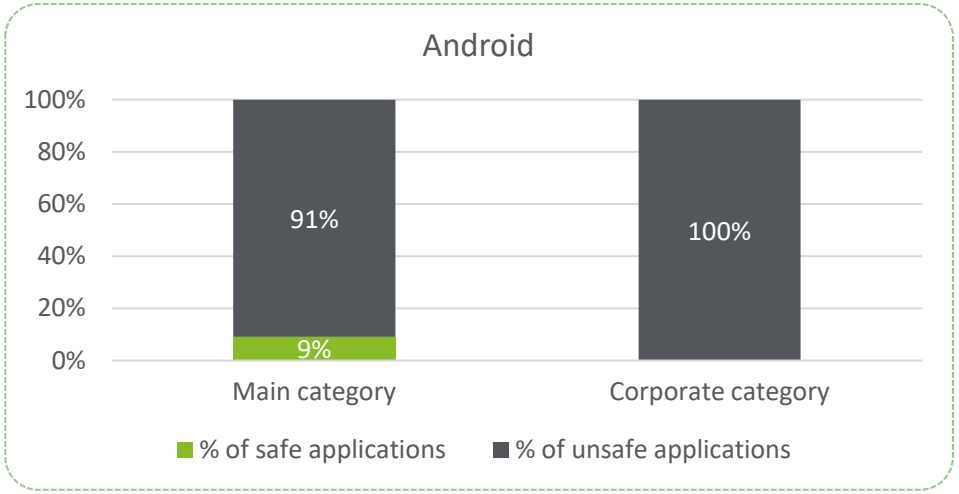
To display apps running in the background on a mobile device, the built-in Android or iOS engine takes an automatic screenshot of the app screen when switching. This standard functionality potentially poses a privacy risk, as critical data can be captured on the screenshot. These, in turn, are stored in local storage and remain unchanged until the app is closed.

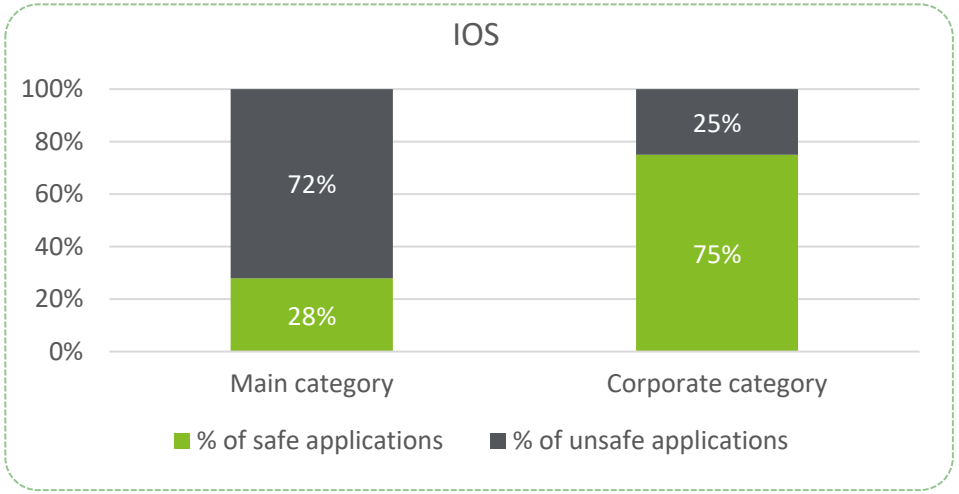
In practice, there are spyware programs that are often installed by the user, which collect screenshots of background applications and then send them to an intruder. To protect confidential information from this type of threat, developers resort to various tricks, such as blurring the image on a screenshot, making it impossible to understand or replace it with a standard one that does not display any confidential data.

To check whether the application prevents you from taking screenshots or recording the screen of the device, we checked whether it is possible to take a screenshot, as well as whether it is possible to disable this lock in application settings.

The study for Android devices found that the security score for "main" category applications was 9%, which is quite low. At the same time, applications in the "corporate" category were 100% unsafe.

When testing mobile apps for IOS devices, the mobile app's screen capture protection score for the "main" category was 28%, while the result for the "corporate" category was 75%.





9. Mobile banking security

9.3 Checking safety mechanisms

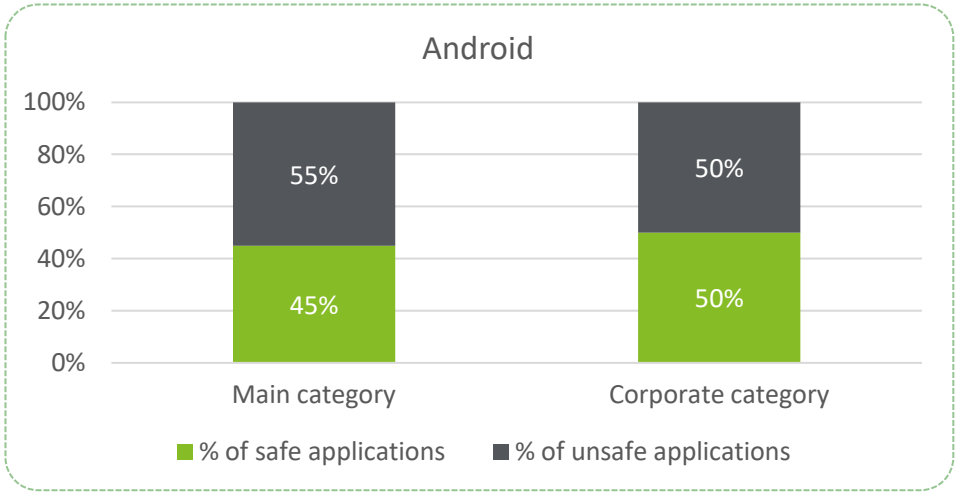
Given that banking applications are designed to process sensitive financial information, developers are advised to take care of the security of both the stored information and the security of the applications themselves. This can be achieved by implementing a full list of security mechanisms aimed at reducing risks. For example, automation of the following basic system environment checks:

- Starting a mobile device with privileged access ("root detection").
- Detecting a program launch in a virtual environment (supports ARM-based startup only).

Violation of one of the above requirements must result in the inability to start the application or significantly limited functionality.

If an application refused to run on an emulator, it was checked whether it could run on a real device with the ability to hide root rights. If the app was launched with root access denied, the app was categorized as unprotected.

This test was conducted only for Android apps, and results showed that the vulnerability rate of the "main" category was 45%. The results for apps in the "corporate" category were also disappointing, as only 50% of apps were protected against this type of attack.



9. Mobile banking security

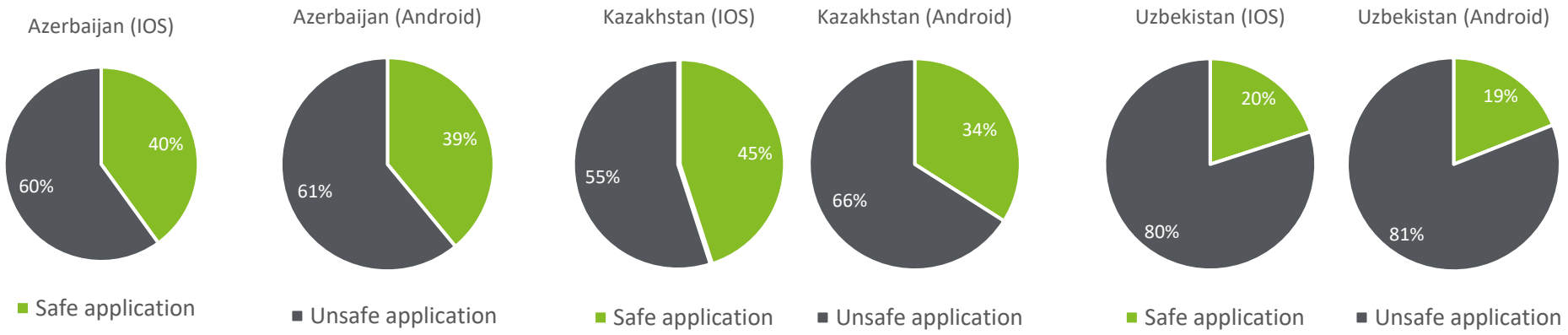
Conclusions

Modern mobile platforms (Android and iOS) have a rich set of built-in security mechanisms. However, very often developers, in the rush to launch a new release, make unforgivable mistakes in terms of protecting the application and the data it processes. Unfortunately, this often results in vulnerabilities that cybercriminals are bound to exploit.

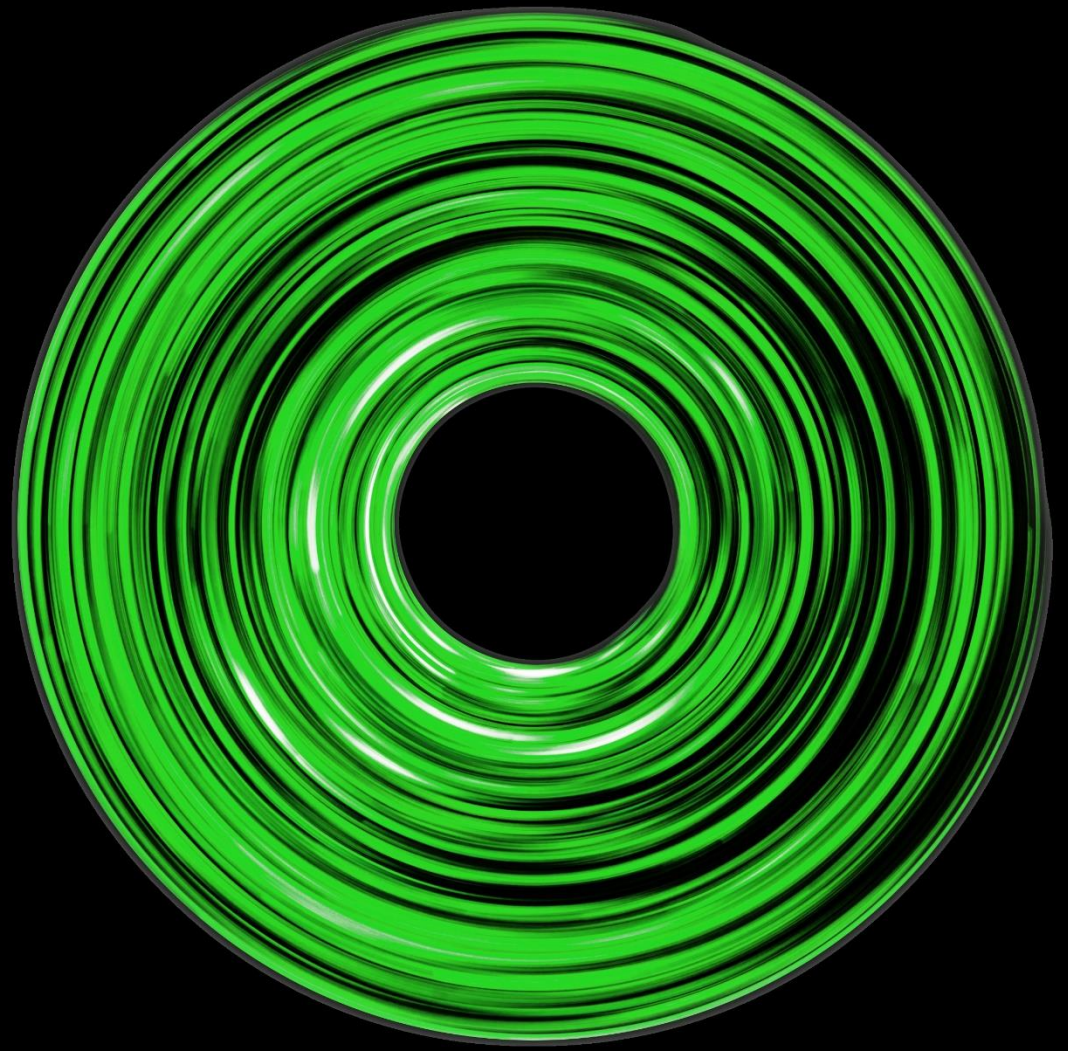
One of the most interesting observations from research in this domain is that the common perception that "iOS" is more secure than "Android" can be misleading. In practice, the level of device security depends not on the platform but on the literacy and competence of the developer, in our case the banking application developer or group of developers. We can talk about application security for the end user only if the developers follow all the recommendations for secure development and implement all the necessary protection measures without exception.

For all countries, the level remains very low. Given the current trends, this situation is a key challenge for the entire banking sector in the region. After all, in the foreseeable future, the share of both mobile clients and banking services provided via cell phones is most likely to grow.

Summarized mobile banking security results by country:



10. Log4J vulnerability



10. Log4J vulnerability

In late 2021, a critical vulnerability was discovered in Log4j versions 2.0.0 and up to 2.15.0. As an Apache logging library, Log4j is responsible for logging events - errors as well as common system operations and transmitting diagnostic messages about them to system administrators and users.

The vulnerability discovered allows users to specify their own code to format a log message. As a result, an attacker can use the vulnerability to steal data and download additional malicious code installing malware.

Given that this library was used by many software solution developers around the world, it was decided to include the analysis of this vulnerability in the scope of the current study.

The results of the study showed that none of the Azerbaijan bank websites are affected by this vulnerability.

100%

of websites are not vulnerable to Log4Shell

10. Log4J vulnerability

Conclusions

One of the major issues with Log4Shell is Log4j's place in the software ecosystem. Logging is a fundamental function of most software, which makes Log4j extremely common. In addition to popular games such as Minecraft, it is used in cloud services such as Apple iCloud and Amazon Web Services, and a wide range of programs, from software development tools to security tools.

Azerbaijan and Uzbekistan bank website showed 100% immunity to Log4Shell, and only one bank in Kazakhstan was found to be vulnerable.

To reduce the risks associated with the existence of this library in software products used, we recommend using the following instructions: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Summarized results of Log4j vulnerability for all website categories:

100%
of all websites in Azerbaijan
are not vulnerable to Log4Shell

98%
of all websites in Kazakhstan
are not vulnerable to Log4Shell

100%
of all websites in Uzbekistan
are not vulnerable to Log4Shell

Deloitte.