Deloitte.

Azerbaijani banks cyber security review

Cyber Risk Advisory

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Deloitte in Azerbaijan has performed its first Cyber Security Survey, during which it analyzed the public web resources of 26 Azerbaijani banks. To conduct this review, utilized set of publically available online tools such as Google, Barracuda, TrustedSource, Haveibeenpwned and others. Current situation in the following eight cyber security areas was assessed:

1. Availability
2. Domain reputation
3. HTTP Headers
4. TLS and SSL
5. Email leaks
6. Open ports
7. Cybersquatting
8. GDPR Compliance.

Information for each area mentioned above were collected, validated and analyzed by Deloitte's Cyber team. All observations in the report accompanied with short description of findings and explanation of the cyber risks associated. All areas have corresponding conclusion where provided recommendations to address related risks.

To determine whether banks will address identified vulnerabilities and improve security of their web resources, we plan to conduct reviews similar to this one on a regular basis.

We hope you will find the report useful. However, in case you will have any comments or issues in regard of information stated here please contact us.

Warm regards,

Vladimir Remyga
Cyber Risk Advisory
Baku, Azerbaijan

Vladimir Remyga
Director
Cyber Risk Advisory

telephone: +994 12404 1210
mobile: +994 51206 0123
+7 700 714 5505
e-mail: vremyga@deloitte.com

Executive Summary

Today, most of Azerbaijan's banking executives are putting significant resources into digital transformation, which is part of their long-term strategy to improve efficiency. This means that more and more emerging technologies are entering our everyday lives—mobile and internet banking, remote money transfers, payments, and other tools are now commonplace in Azerbaijan.

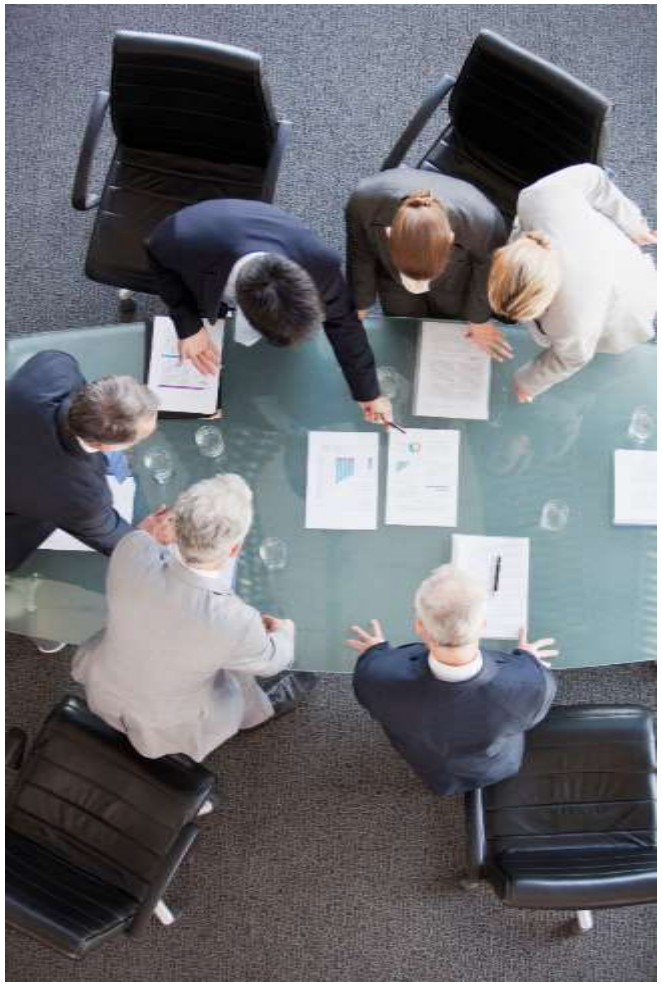
However, our review reveals that not all cyber leaders at banks are aligned when it comes to steering the best course to protect infrastructure.

Many banks do not follow standard security best practices when they set up their web servers. As a result, even without using specialized software, we have identified important deficiencies at a number of banks. What's more, a large number of these were not new problems or zero-day breaches, but rather fairly old and well-known cyber security issues. Although these deficiencies may seem insignificant, they can lead to leaks of confidential financial data or direct theft of funds from client accounts.

At same time there are cases when we seen lack of banks employees awareness in cyber security matters. It is an indication of weakness existing cyber security policies and cyber education programs applied in banks. In fact one ill-fated click from an unknowing employee could threaten the entire bank's data.

On top of that the COVID-19 crisis has put extreme economic strain on many organizations, and banks as well. Thus they have to adjusting to the "next normal." With significant amount of employees working from home, business executives focused solely on maintaining operational capacity and functionality at all costs. However, if cybersecurity is not built into their tactical and strategic plans, banks could be seriously compromised in the short-term.

More important than ever before, Azerbaijani banks need to embrace a "cyber everywhere" reality and view it as the connective thread that weaves their internal organization, customers, vendors, and communities together—enabling them to integrate cyber into decisions their management makes every day.



About Deloitte Cyber

Deloitte Cyber helps organizations perform better, solving complex problems so they can build smarter, faster, more connected futures—for businesses, for people, and for the planet.

As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategies and investments with strategic business priorities, improve threat awareness and visibility, and strengthen clients' ability to thrive in the face of cyber incidents.

Using human insight, technological innovation, and comprehensive cyber solutions, we manage cyber everywhere, so society can go anywhere.

Why Deloitte

Our heritage, built on deep technology expertise, broad industry experience, and a comprehensive suite of solutions, covers every aspect of cyber risk management. In addition, we:

- Push the boundaries of cybersecurity risk strategy and create new avenues for innovation by partnering with global leaders
- Develop new knowledge for cyber risk and upscale the industry by cultivating best-in-class expertise
- Strengthen cyber risk standards for organizations worldwide by investing in cutting-edge technology
- Make a bigger impact on our client's operations to drive progress by offering a comprehensive suite of solutions across strategy, implementation, and managed services
- As new technologies emerge and connectivity increases, Deloitte Cyber Risk is uniquely positioned to help our clients navigate this complex and uncertain landscape.

1. Availability
2. Domain reputation
3. HTTP Headers
4. TLS and SSL
5. Email leaks
6. Open ports
7. Cybersquatting
8. GDPR Compliance

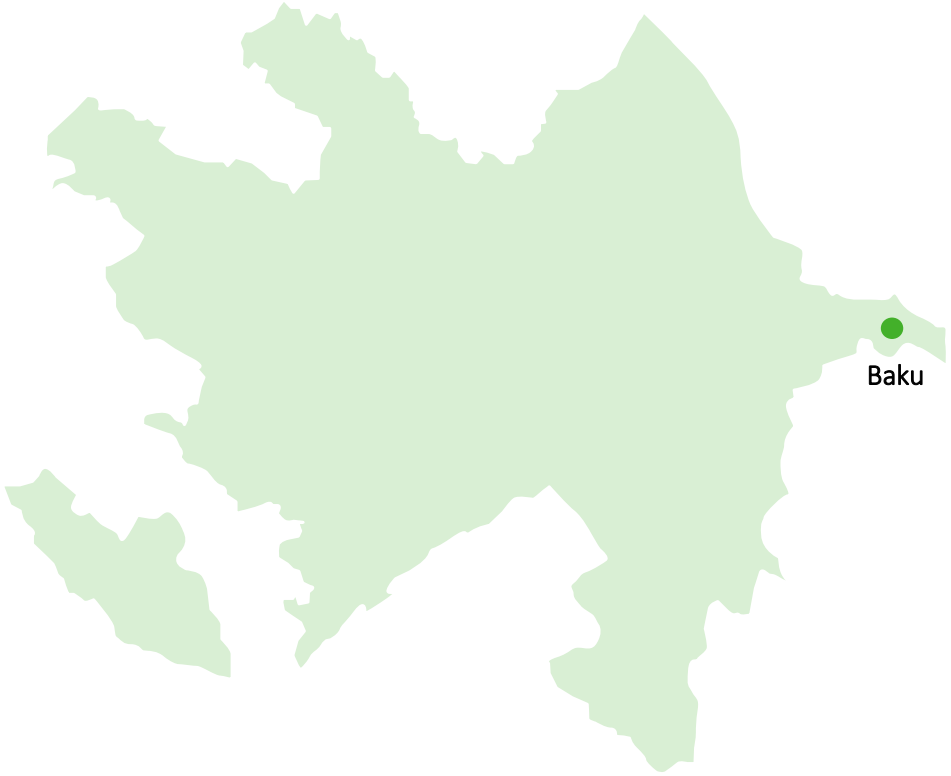
Deloitte in Azerbaijan

Deloitte is represented in the largest city-capital of Azerbaijan, Baku, where over 140 of our specialists are employed.

Deloitte in Azerbaijan is part of Deloitte CIS Holdings Limited (“Deloitte CIS”), a member firm of Deloitte Touche Tohmatsu Limited (DTTL).

We provide audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries through over 3,800 people working across 9 CIS countries, Georgia and Ukraine.

Deloitte CIS is represented in Russia (Moscow, St. Petersburg, Ufa, Ekaterinburg, Novosibirsk, Vladivostok and Yuzhno-Sakhalinsk), Ukraine (Kyiv), Belarus (Minsk), Georgia (Tbilisi), Armenia (Yerevan), Azerbaijan (Baku), Kazakhstan (Aktau, Almaty, Nur-Sultan, Atyrau), Kyrgyzstan (Bishkek), Uzbekistan (Tashkent), Tajikistan (Dushanbe) and Turkmenistan (Ashkhabad).



Contents

Availability

1. Availability

01

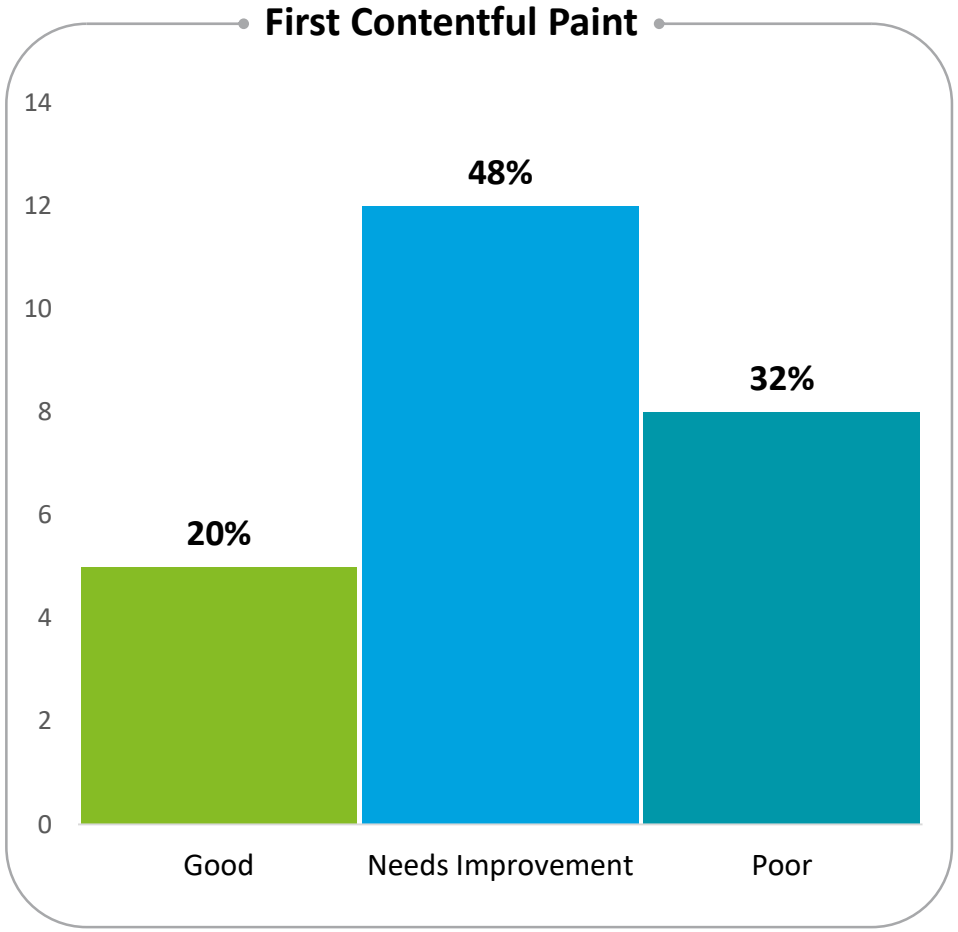
The performance of banks' websites plays a key role in their availability during denial-of-service attacks. While there are numerous ways of assessing website performance, in this study we have used the following metrics: First Contentful Paint (FCP), Response Time, and First Input Delay (FID). The first two are based on timing server-client information exchange, while the last measures the performance of websites on the client side.

1. Availability

1.1 FCP

First Contentful Paint, introduced by Google, measures the time it takes to paint any content in a browser window after a user's website request. It is measured in seconds, and the lower-the-better rule is applied to results. In our tests, we used Google's PageSpeed web resource, and timing values were interpreted using the ranges stipulated by Google’s official performance scoring method. Results were also compared with the median values of a selection of leading global banks to obtain a general picture of the state of the industry.

According to our tests, 20% of bank websites were Good, 48% were rated Needs Improvement, and 32% were Poor. However, when compared with their leading global peers, 58% of local banks displayed results that were above the median value representing good practice.



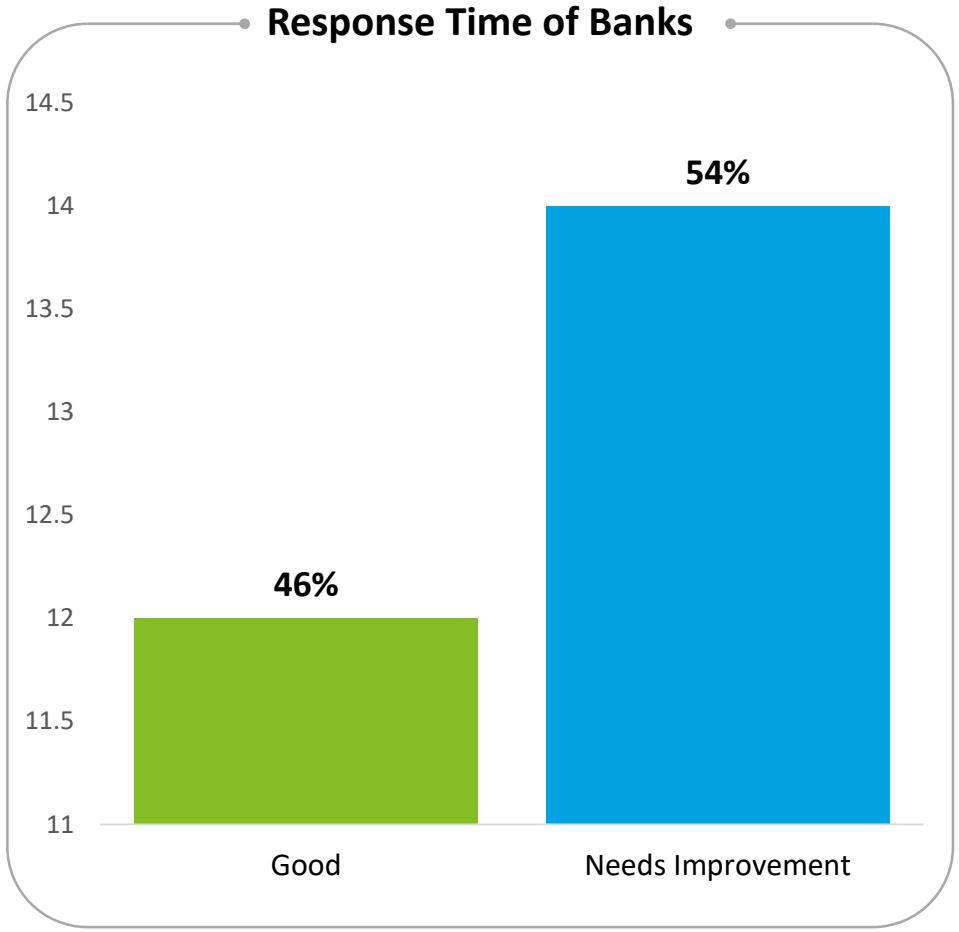
1. Availability

1.2 Response Time

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

To measure RT values, we used the K6 online load testing tool. Testing configuration included 20 virtual users (VUs) from Europe 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. Each result value was interpreted by comparing it to the upper limit of best practice: 500 milliseconds.

Only 46% of the banks we tested had a website with a Good response time, while the remaining 54% were rated Needs Improvement.



1. Availability

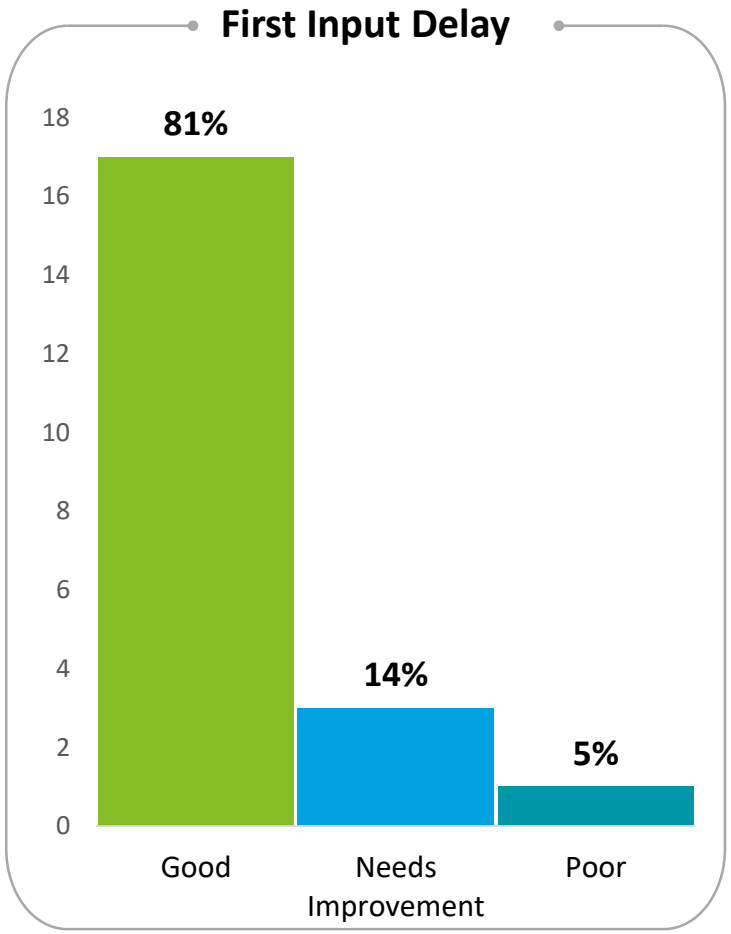
1.3 FID

First Input Delay, introduced by Google, is a relatively new metric that allows websites to assess client-side performance. FID indicates the time taken by a browser to process the first user input on the website and display the corresponding content. It is measured in milliseconds, and the lower-the-better rule is applied here as well. A high FID time may be an indicator of poor website optimization or an inordinately large amount of code or content, which can result in a poorer user experience or speed downgrade.

Similarly to FCP, we used Google's PageSpeed web resource, and the time values were interpreted using the ranges stipulated by Google's official performance scoring method. Results were also compared with the median values of a selection of leading global banks to obtain a general picture of the state of the finance industry worldwide.

We established that 81% of the banks we tested had a Good FID rate and 14% Needed Improvement; only 5% were rated Poor.

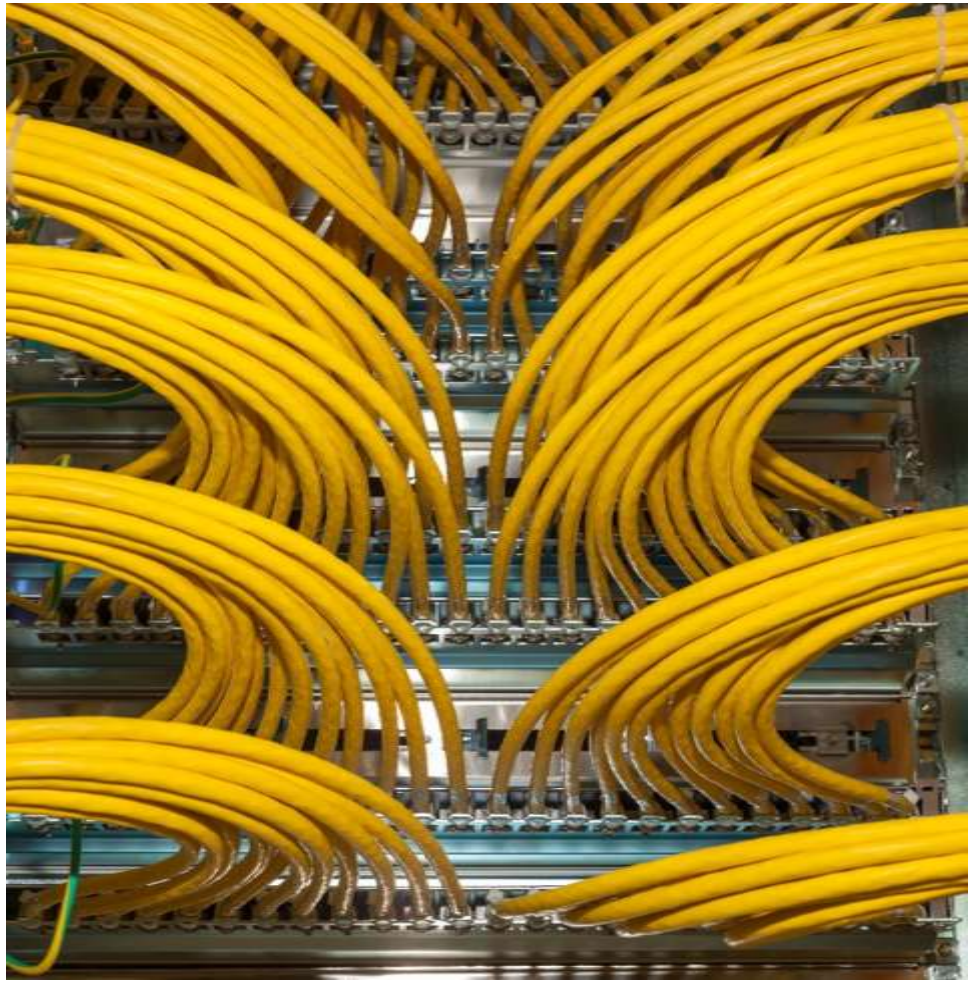
Although the results we collected may seem acceptable, 50% of local banks were below the target median value compared with their leading global peers.



1. Availability

1.4 Conclusion

Although the benchmarking spotlight revealed that about 50% of local banks follow good practices, some performance challenges remain, most notably from Google, a key IT player, according to which the performance of a significant number of Azerbaijani banks needs improvement or is poor.



Domain reputation

2. Domain reputation

02

Domain reputation plays a crucial role in trust relations in cyber space. And ever since email providers and search engines have started relying on information from domain reputation providers, the importance of this factor has only increased. Emails sent from the domains of banks that have low reputation scores, or ones that have been blacklisted by web reputation providers, may be indexed as spam by mailbox providers, and their web resources could fail to appear in search engine results.

Below, we present the results of our domain reputation analysis of Azerbaijani banks, which was conducted using four web reputation providers: Talosintelligence, TrustedSource, ReputationAuthority and Barracuda Reputation System.

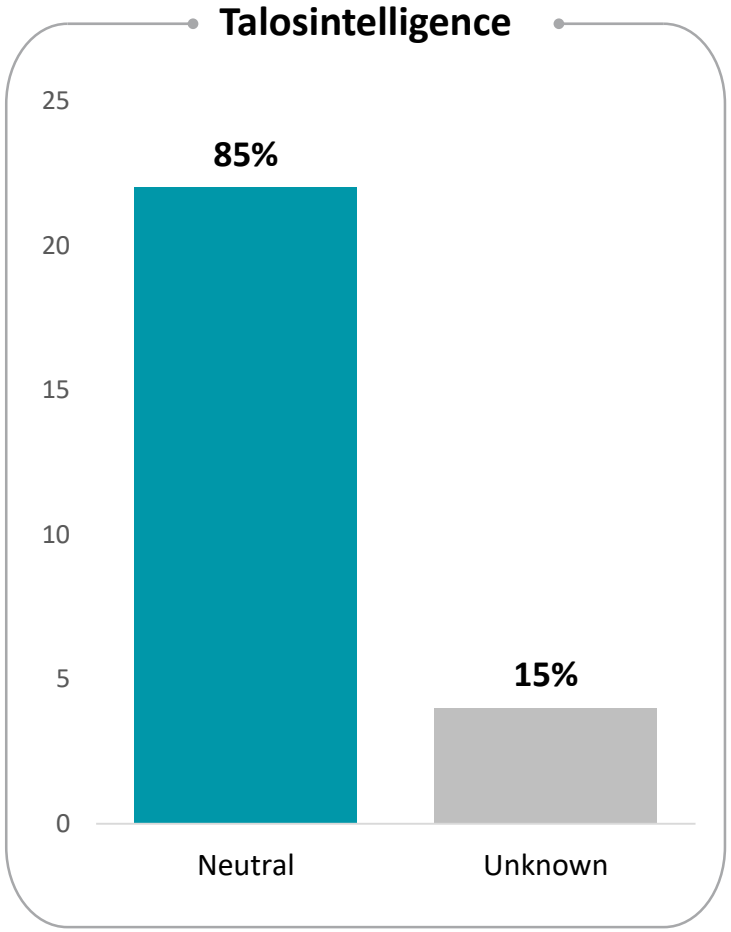
2. Domain reputation

2.1 Talosintelligence

Talos Intelligence provides domain reputation services powered by Cisco. It detects and correlates threats in real time using the largest threat detection network worldwide, covering emails, web requests, malware instances, data sets, endpoint intelligence and network intrusions. Cisco solutions rely on domain reputation verdicts provided by Talosintelligence as the first filter for incoming traffic to offload operating performance. Other solutions may also rely on Talos Intelligence reputation indicators.

Talos categorizes domains' reputations into four groups: Trusted, Neutral, Untrusted, and Unknown. Before assigning a Trusted reputation to a domain, Talos collects substantive positive evidence about it over time. This means that most domains have a Neutral reputation. An Unknown reputation is assigned when the resource has not been evaluated yet or there is not enough information to issue a threat level verdict.

According to our assessment, no bank in Azerbaijan has a Trusted domain. However, 85% of local bank domains are evaluated as Neutral. The remaining 15% have Unknown reputations



2. Domain reputation

2.2 ReputationAuthority

This service provides domain reputation data powered by WatchGuard, a cyber-security technology provider. ReputationAuthority monitors and publishes IP and domain names connected with malicious or unwanted email and web traffic received from security appliances.

Domains receive a reputation rating independently from the IP address or other domains outbound from the same IP address.

WatchGuard solutions rely on domain reputation verdicts provided by ReputationAuthority as the first filter for incoming traffic to reduce unwanted network traffic. Other solutions may also refer to ReputationAuthority reputation indicators.

ReputationAuthority domain reputation verdicts comprise three overall scores: Bad, Neutral, or Good. As with Talos, ReputationAuthority collects substantive positive evidence over time before assigning a Good reputation to a domain.

According to our assessment, only 4% (one domain) of local Banks had a Good reputation; the remaining 96% had a Neutral one.

2. Domain reputation

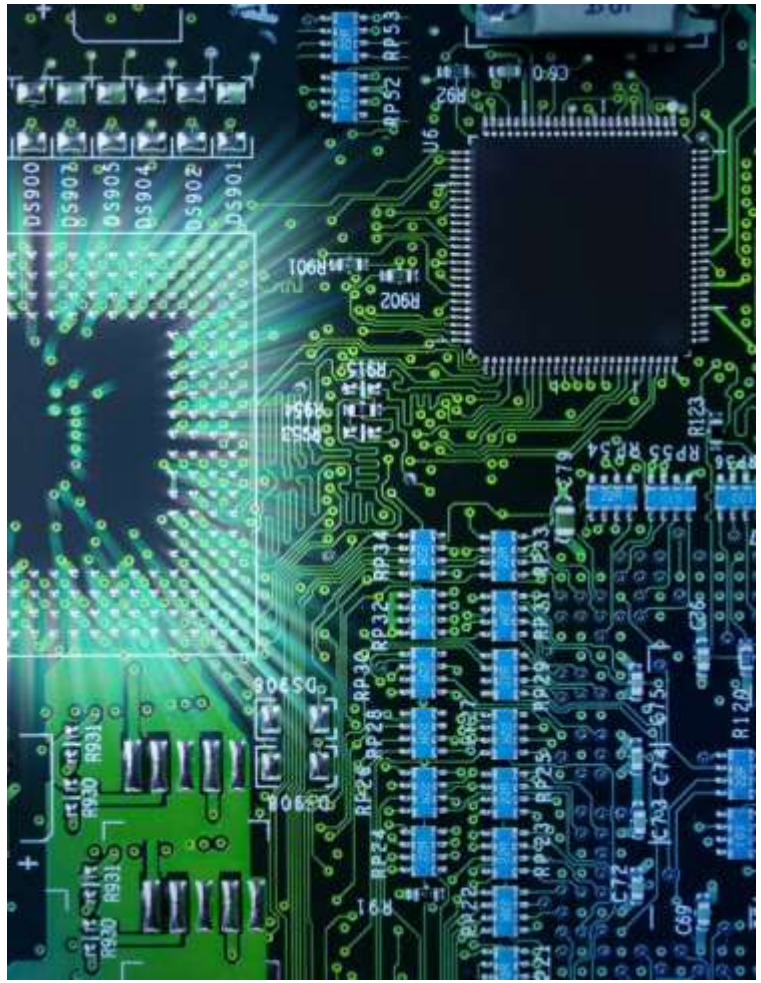
2.3 Barracuda Reputation System (BRS)

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 throughout 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.

Barracuda Central solutions rely primarily on domain reputation verdicts provided by BRS as the first filter to block network-based attacks sent via email, web, and other protocols. Other solutions may also refer to BRS reputation indicators.

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 local Banks have a Good reputation and have not been blacklisted.



2. Domain reputation

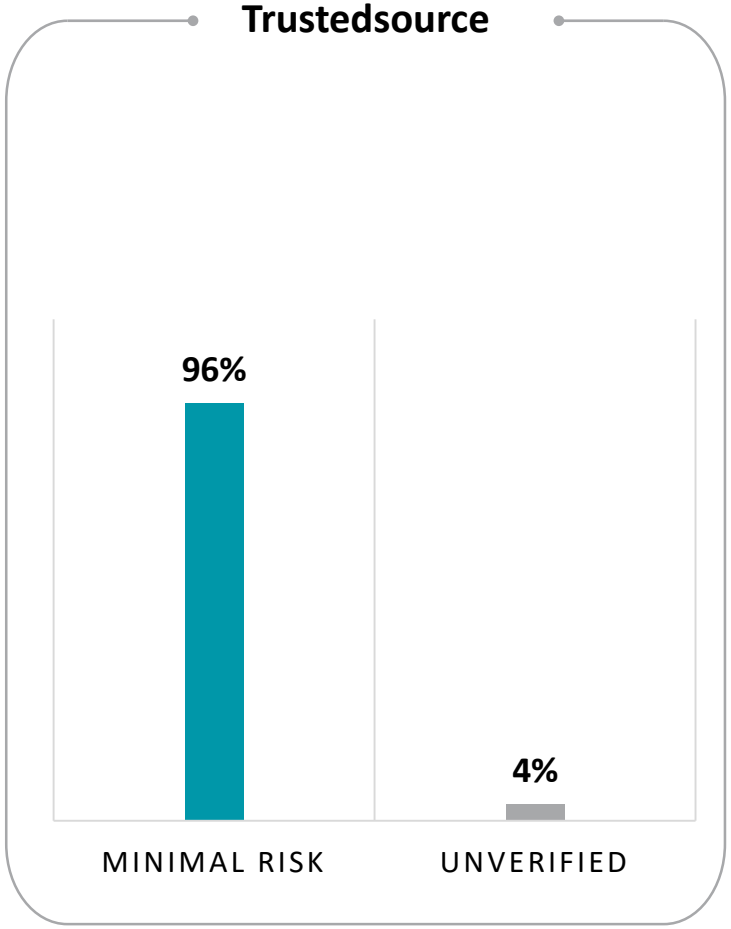
2.4 TrustedSource

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 local banks have Minimal risk reputations, and the remaining 4% (one domain) has an Unverified reputation.



2. Domain reputation

2.5 Conclusion

Analisys of the domain reputation of Azerbaijani banks shows that no domains have a weak or negative reputation. This means that their domains haven’t 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.

HTTP Headers

3. HTTP Headers

03

Website security covers a wide range of measures, and violating the integrity of just one component may lead to the entire site being hacked. Even if an attacker does no more than deface a site’s main page, without managing to steal funds from customers' accounts or obtain confidential information, significant indirect losses or damage to the brand's reputation may ensue. This is why it is so important for banks to comply with all aspects of security in order to fully protect their Internet resources.

In this part of the report, we have limited our analysis to just one of the many areas that must be efficiently managed to properly protect websites: the security settings of HTTP headers. Bad actors can easily take advantage of the fact that information about HTTP headers is publicly available to compromise banks websites, making the proper configuration of settings imperative.

3. HTTP Headers

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 logic of this attack is very simple: a website user clicks on one element of the page, but actually interacts with another. This can be realized in different ways, but making a frame transparent and adding it to the original content, thus forcing the user to click on the area, is the most common approach. As soon as a user clicks on the transparent (colorless and invisible) frame, the clickjacking is complete. In the context of the banking industry, this may cause the user to make a quick payment that does not usually require confirmation. Organizations can find out whether their website is vulnerable to clickjacking by adding their existing page link to iframe with a simple HTML.

This example demonstrates the importance of protecting websites from clickjacking attacks, and X-Frame-Options headers are an effective preventive measure.

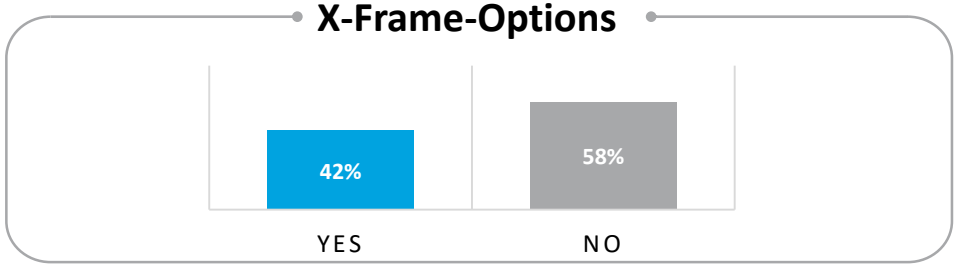
Three basic options are allowed for X-Frame-Options headers:

1. DENY: restricts the current page to be displayed within an iframe;

2. SAMEORIGIN: allows the current page to be displayed only in the current area within another page;

3. ALLOW-FROM URL: enables the current page to be displayed within another page, but only in the specified URL, such as www.sample.com/frame-page.

Our assessment of local banks with regards to the existence of X-Frame-Option headers revealed that 42% of banks had server-response restrictions for this header. However, the remaining 58% did not apply this restriction.



3. HTTP Headers

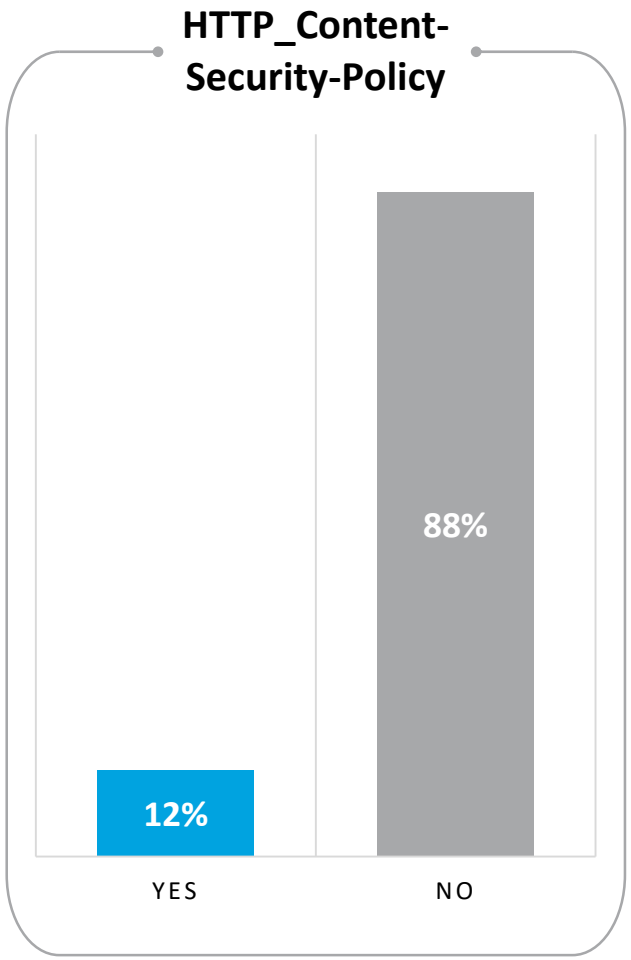
3.2 Content-Security-Policy (CSP)

SP headers allow organizations to restrict the acceptable sources of website content. CSP can be seen as an additional security layer or browser security standard that grants the ability to create instructions regarding which areas, subdomains, and resource types can load from a particular web page. CSP helps load JavaScript resources from a specific area, also preventing inline JavaScript from running on the site. This allows XSS, Formjacking, and SQL Injection attacks to be detected and prevented. Another advantage of using CSP is the ability to quickly learn about new XSS attacks. Using the report-url option, the browsers of the attacker and victim will send reports to the specified URL as soon as the CSP is triggered.

The whitelisting approach is used when defining rules in CSP. This allows organizations to specify the resources they accept while preventing the use of others; they only need to list the resources that will be included in the CSP. Besides HTTP headers, CSP rules can also be added to the HTML tag.

That said, website administrators must consider the settings of CSP rules carefully, as invalid configurations may lead to resource unavailability and an illusion of safety.

According to our assessment, only 12% of local banks are using CSP headers as part of their web server's response. The remaining 88% do not use this security feature.



3. HTTP Headers

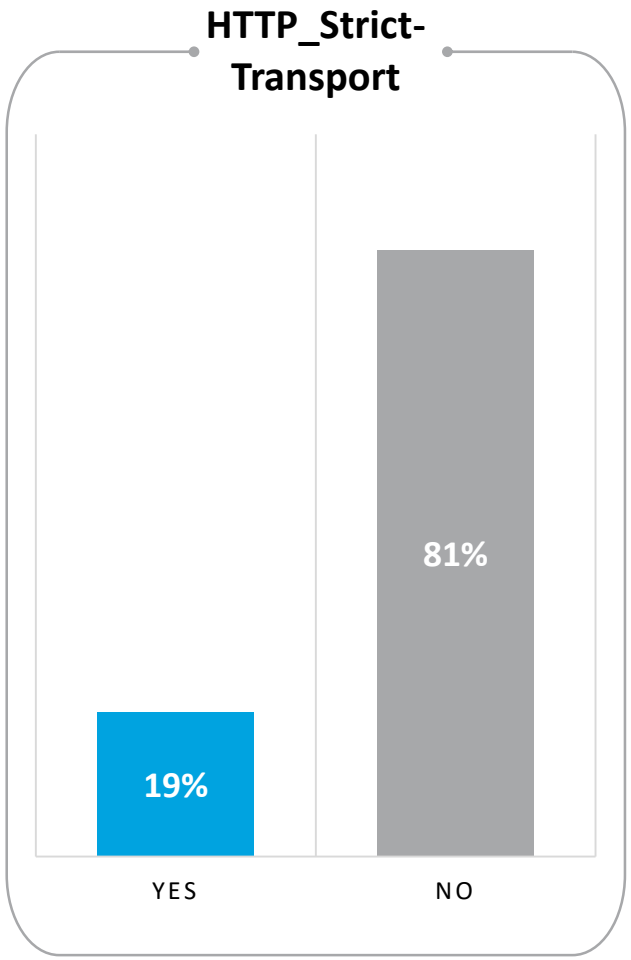
3.3 HTTP Strict Transport Security (HSTS)

This header forces 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.

Imagine you are sitting in your favorite cafe or in a hotel room and want to use the free Wi-Fi. Have you ever noticed that in such places, Wi-Fi passwords are often printed on paper (a notepad, brochure, card, etc.) and have never been changed? Malicious hackers can easily connect to public networks, allowing them to view and manipulate the data of anyone using that network. Hackers are able to capture network traffic over insecure HTTP for any website by using 301 Redirect to switch from HTTP to encrypted HTTPS. This method can allow hackers to remove your SSL encryption and steal your personal data, or even worse, grab your login information.

Therefore, bank websites should use only HTTP Strict Transport Security (HSTS) rather than HTTPS. Even if they are using an SSL Certificate and transfer traffic from HTTP to HTTPS using 301 Redirect, full network security is not guaranteed. HSTS ensures a higher level of security.

Despite the fact that HSTS headers are an important way of protecting users from hackers, only 19% of bank servers in Azerbaijan use them. Most banks (81%) do not.



3. HTTP Headers

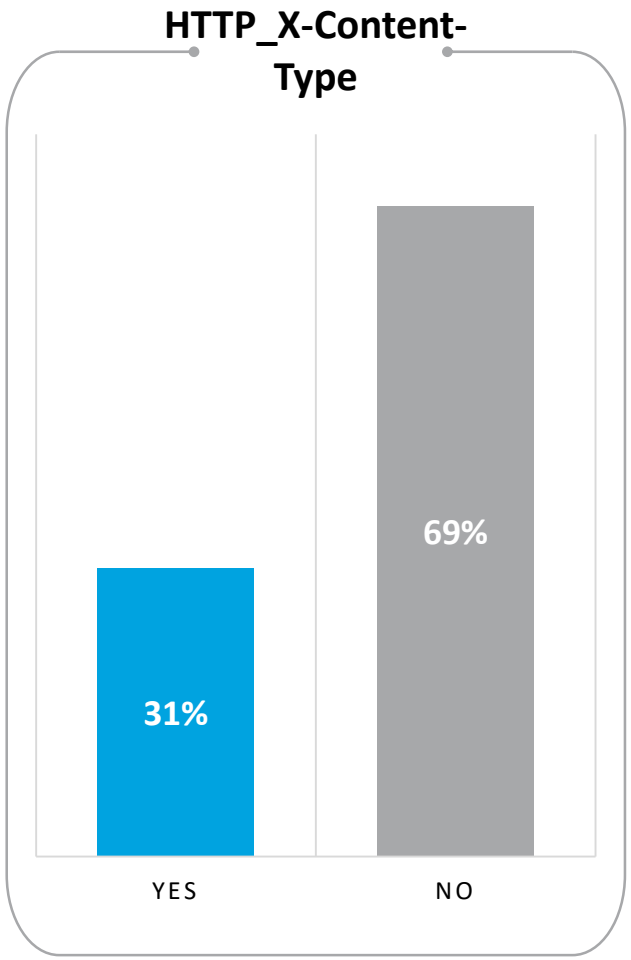
3.4 X-Content-Type-Options

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 don't use it, which means that browsers must determine what type of content type they are consuming. For this reason, browsers have had to implement "sniffing" techniques to detect the type of content when content type headers are not served.

However, this has led to serious security issues. To avoid them, the X-Content-Type-Option nosniff line should be added to the HTTP header to prevent Internet browsers from deciding on content by sniffing 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).

Only 31% of local banks' websites feature the X-Content-Type-Options: nosniff header. The remaining 69% do not use this security feature.



3. HTTP Headers

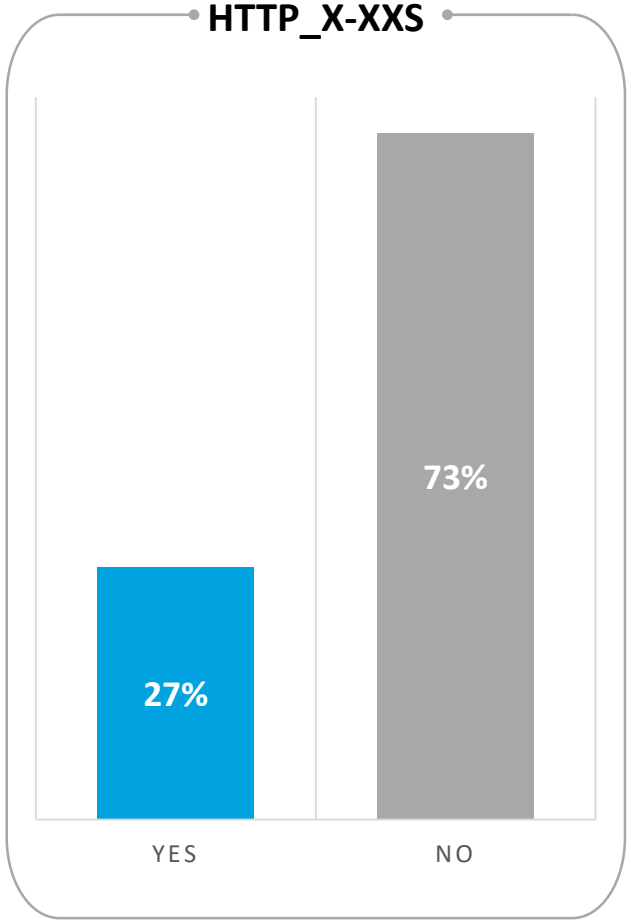
3.5 X-XSS-Protection

This response header protects website users from Cross Site Scripting (XSS) attacks by enabling client-side cross-site scripting filtering.

Modern browsers such as Internet Explorer 8+, Chrome, Edge, Opera, and Safari are able to detect potential XSS payloads by filtering on content. To enable this feature, the X-XSS-Protection response header is used.

Eliminating XSS weaknesses on the application side should be a priority for website developers. After providing code-based security, XSS Protection should be activated in internet browsers to increase the security level.

According to our review, only 27% of local Banks have an X-XSS-Protection header in their server response, while 73% do not use this feature.



3. HTTP Headers

3.6 Set-cookie security flags

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

Cookies can also be used for other purposes besides the session key, such as storing the reference to the last image clicked in the image gallery. In this way, HTTP traffic can be reduced and the webserver can solve some tasks by using the internet browser of the user.

Although this is very useful, organizations still need to understand which cookie values are important for security—namely the value that contains the user ID number (session ID). This value should be used in a secure HTTPS request only; extreme cases are exceptions.

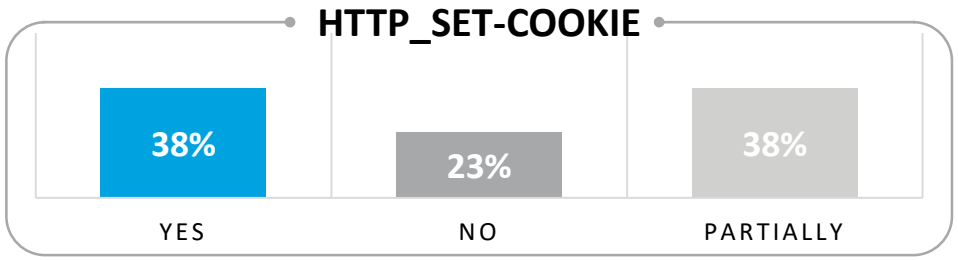
Cookie information can be stolen with JavaScript through attacks such as XSS, for which HttpOnly and secure flags can be used as protection. This helps prevent the theft of cookie information and minimize potential harm.

The HttpOnly flag is a highly effective cookie protection method that prevents JavaScript from reading session cookies. If the HttpOnly flag is set in the HTTP response, the cookie cannot be accessed through the client-side script.

As a result, the browser does not show the cookie to third parties even if there is a cross-site scripting vulnerability and a user accidentally accesses a link that exploits it.

Another area where cookies should be protected is during data transition between client and server, when a bank webserver's page can be accessed by both HTTP and HTTPS. HTTPS traffic is end-to-end encrypted, while it is unencrypted with HTTP. To protect the session information from the cookie file, only HTTPS should be used. This can be achieved by adding a secure flag to the set-cookie header.

According to our assessment, 38% of local banks use both HttpOnly and secure flags, while another 38% use only one of them; the remaining 23% do not use any.



3. HTTP Headers

3.7 Public-Key-Pins

This response header can pin the fingerprint of the web server's public key in the browser, and the browser will not accept certificates from other public keys. This can prevent the webserver's clients from attacks with fake certificates.
In order to understand the logic of public key pinning, it is necessary to know what secure connections offer and how they work. When users want to access a website safely, the server sends its own public key, which is then used to encrypt incoming traffic to the server from users. This certificate contains information such as the name of the site, how long the certificate will be valid, and how many bits of cryptographic keys are being used.
Certificates also contain an additional piece of information: the name of the Certificate Authority (CA). When public key information is sent to clients, the browser must ensure that a website is authentic. To do so, it checks with a CA, which is a trusted third-party company that signs webservers' certificates. This information is contained within the certificate. Based on information from the CA, browsers can prove the authenticity of a webserver's certificate. If no problems are found, browsers continue to communicate with the webserver securely.
Unfortunately, malicious activity is common in cyber space. Based on their own experience and recent events, cyber specialists know that it is possible for a CA to sign a certificate on behalf of another website. This mostly happens as a result of hacker attacks on CAs.
HTTP Public Key Pinning (HPKP) was created to prevent attacks featuring signed fake certificates. Using this feature, websites can report their fingerprints (the hash values of their certificates) to browsers with a Public-Key-Pins response header. If a website claims to own a certificate other than the ones specified, the browser will refuse to establish a secure connection, or even report it to the URL in question.
The HPKP feature protects users and websites in cases when a CA has been compromised or hacked to sign fake certificates.
According to our assessment, only 4% (one domain) of local banks have the Public-Key-Pins header in their server response, while 96% do not use this feature.
The Expect-CT response header declares to browsers that the server has received the certificate through a publicly available CA (the Certificate Transparency Log). This is a relatively new header that is meant to replace HTTP Public Key Pinning (HPKP); it is designed to protect website users from attacks with fake certificates.
Google first accepted Certificate Transparency (CT) logs technology as mandatory in April 2018. As of November 23, 2020, there have been 11,266,751,018 entries made to the set of CT logs that Google monitors. CT technology depends on three operations:
First, for each certificate signed as of April 2018, the CA must add a record to the publicly available Certificate Transparency log.
Second, website owners must engage in monitoring and supervision. It is their responsibility to add the Expect-CT header to the server response. Once scans and alarm systems have been put in place in the CT log system, they are able to see and can be informed of whether a website's certificate has been signed by a CA.
Third, using information in the CT log, browsers must also check to see if the certificates they receive from websites meet requirements.
According to our assessment, only 8% of local banks have the Expect-CT header in their server response, while 92% do not use this feature.

3. HTTP Headers

3.8 X-Powered-CMS and X-Powered-By

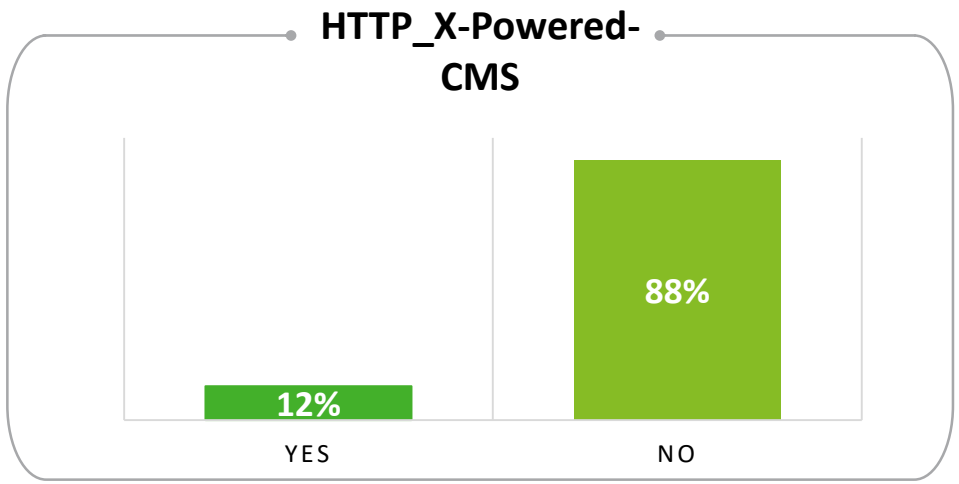
The X-Powered-CMS response header provides the name and version of the Content Management System that generated the server response, such as Bitrix or Express. This response header also provides information on the technology behind a website. It is often added by default in server responses constructed using a specific scripting technology such as ASP.NET or PHP.

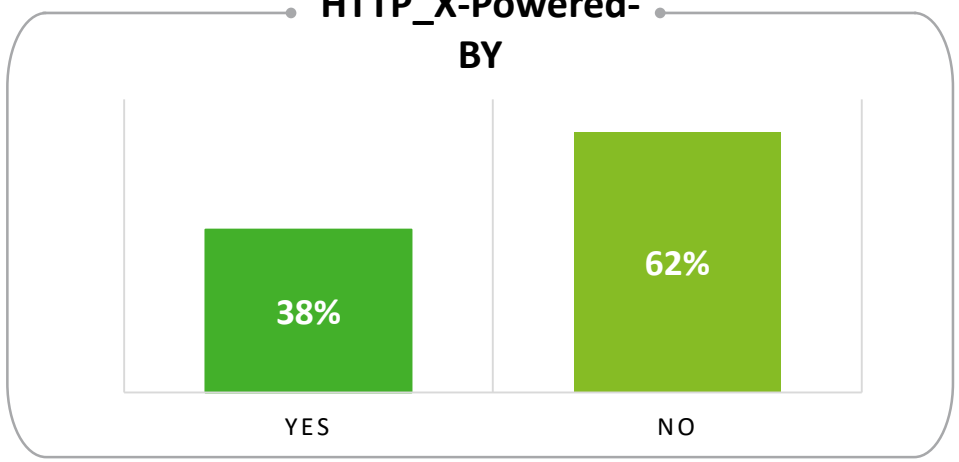
This information does not pose a serious risk if a website's software is regularly updated. However, if possible, it is better to hedge and prudently hide names and versions of technologies from prying eyes, as not doing so can reduce the time required by attackers to collect information and determine subsequent attack vectors.

In our assessment, modified header values were ignored and not counted.

When we checked whether X-Powered-CMS headers were in place, we found that 12% of local banks had default values for this header in their server response, while 88% of websites had removed or modified it.

Meanwhile, 38% of local banks had default values for the X-Powered-By response header, while 62% had removed or modified it.





3. HTTP Headers

3.9 X-Powered-CMS and X-Powered-By

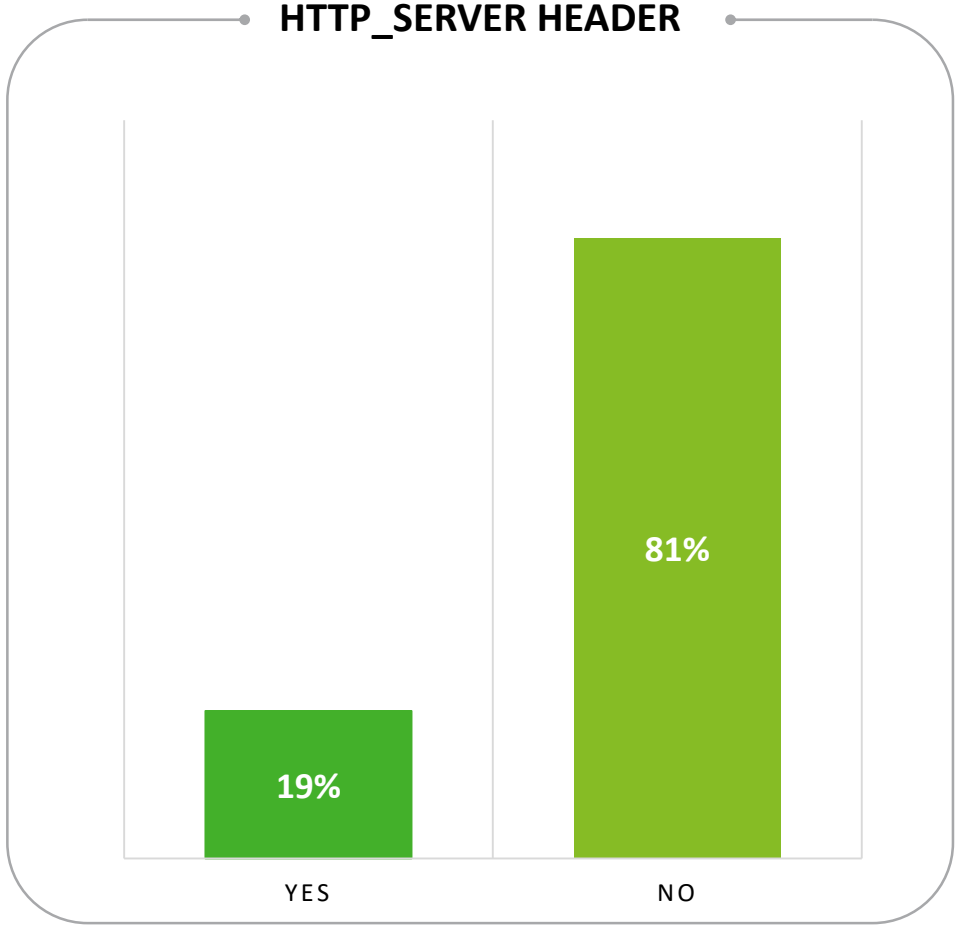
The server response header provides information about the software used by the origin server to handle requests.

Common sample values include nginx/x.x.x, Apache/x.x.x, and Microsoft-IIS/x.x.

Disclosing this information does not pose a direct threat, but it may shorten the time needed by attackers to collect information and determine subsequent attack vectors.

In our assessment, modified values of server headers were ignored or not counted.

Our review of webserver responses revealed that 19% of local banks show the software they use in server responses, while 81% have removed or modified the header value.



3. HTTP Headers

3.10

Conclusion

Setting up and maintaining website security is a complex task that includes a number of areas, and an integrity breach in any of them could be fatal for the entire application and the corresponding data. For this reason, HTTP headers security should not be ignored.

Our analysis shows that most Azerbaijani banks see HTTP headers as minor factors, and they are not using this inherent capability well. This means that in many cases, connected security risks are not mitigated.

HTTP headers are a good starting point for properly protecting websites, as most of them are not too difficult to incorporate. Keeping up with HTTP security header best practices provides an additional security layer on top of any web assets.

TLS&SSL

4. TLS&SSL

4.1 SSL Labs

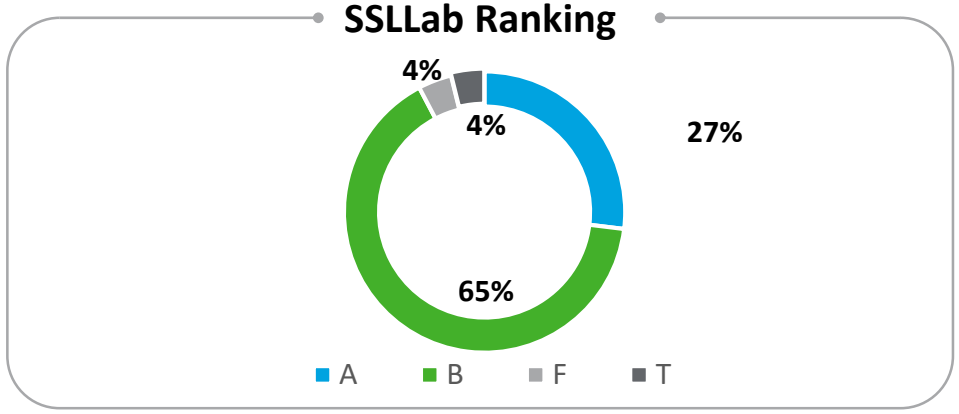
Today, both consumers and companies are choosing services and partners based on HTTPS, which is the secure version of the common HTTP protocol for accessing web resources. In HTTPS, data is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). These cryptographic protocols are the most popular methods of ensuring secure communications over the Internet today.

To make an SSL/TLS connection, the server must have an installed digital certificate confirming the authenticity of the domain and site ownership. This is necessary to ensure that users visit the original resource rather than a fake page created by an attacker.

However, the mere presence of an SSL certificate does not mean that the data of site users are completely safe. SSL/TLS features a large number of settings and features that can impact the security of the connection and its clients in various ways. Incorrect settings may allow attackers to intercept and manipulate the data exchanged between the server and the client.

Warnings and restrictions integrated into browsers have made it simple to determine whether a site or service features strong encryption. For the purposes of assessing these settings, we used the Qualys SSL Labs resource, which rates the SSL/TLS settings of web resources on a scale of A+ (best) to F (worst) based on numerous parameters. One more grade, called T, indicates that the webserver uses an untrusted certificate, which may be caused by an outdated or revoked certificate. Please refer to https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide for the official rating criteria.

Our assessment of local banks' SSL/TLS settings using the SSL Labs resource revealed that 27% have an A grade, 65% a B grade, 4% (one bank) an F grade, and the remaining 4% (one bank) a T grade, which indicates that the resource is not trusted and has poor security settings.



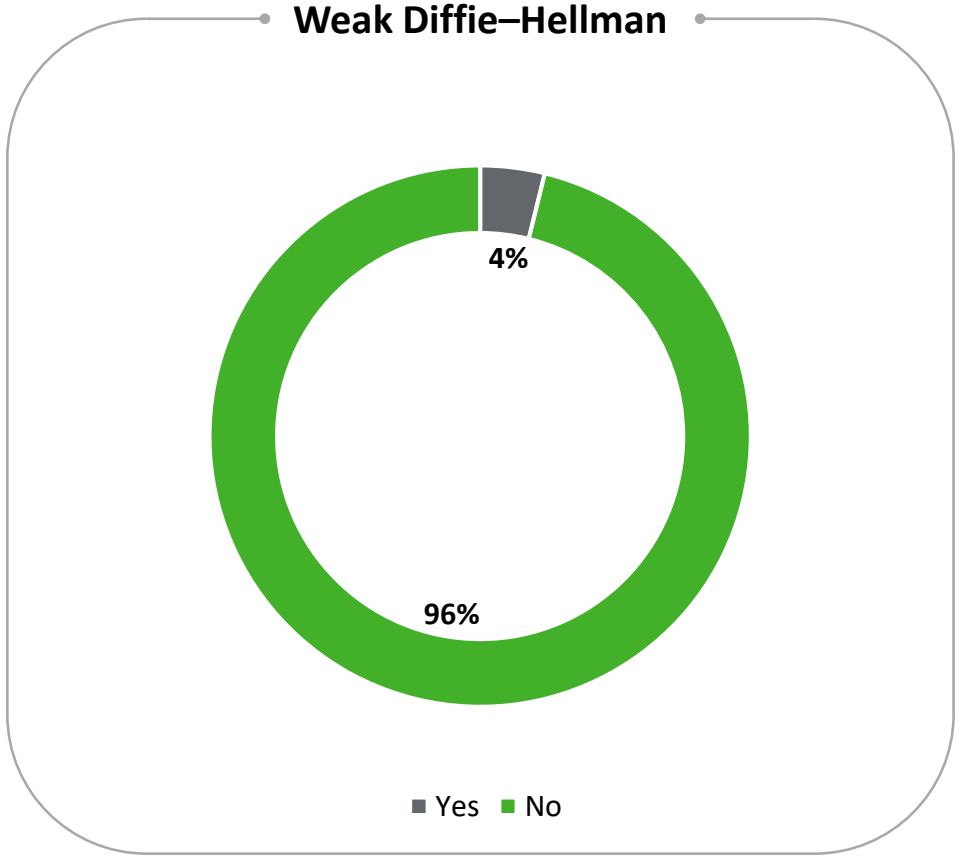
4. TLS&SSL

4.2 Weak Diffie-Hellman parameters

Traditionally, secure encrypted communication between two parties requires an initial key exchange by means of some secure physical channel, such as paper key lists carried by a trusted courier. The Diffie-Hellman key exchange method allows two parties with no prior knowledge of each other to exchange and share a secret key over an insecure communication channel. This key can then be used to encrypt further communications with some symmetric key encryption algorithm.

Websites that use one of the few common 1024-bit Diffie-Hellman groups can be susceptible to passive interception by attackers with appropriate resources. To improve the reliability of key exchange, larger primes should be used, such as, 2048-bit primes. A safer option is to switch to the Diffie-Hellman protocol based on Elliptic curves. Elliptic curves do not suffer from common precomputation problems, which means attacks on parameters that are barely computationally rangeable only compromise one connection, not everyone using that group.

Our assessment of the Diffie-Hellman parameters of local banks revealed that only 4% (one Bank) had weak Diffie-Hellman parameters, while the remaining 96% had a secure parameters set.



4. TLS&SSL

4.3 SSL 2.0 and SSL 3.0 support

Both SSL and TSL are encryption and authorization protocols. With the help of these protocols, data transfer is performed securely from server to server or from server to client. SSL is the more primitive form of TSL. Developments in the information security world over the years have led to the creation of TSL, which is an improved version of SSL. However, some public web resources still support SSL for encryption.

SSL was first published by Netscape in 1995 as SSL 2.0 (the SSL 1.0 protocol, the first version of SSL, was never made available to all users). SSL 2.0, which was on the market for a while, turned out to have serious security vulnerabilities, which led to its replacement in 1996 by a newer version, SSL 3.0. Various vulnerabilities have been discovered in SSL 2.0 and 3.0 since the 90's, some of which were confirmed by IEFT in 2011 and 2015. Many of these vulnerabilities are no longer usable, but the scenarios experienced gave the impression that SSL was not as reliable as it should be.

Internet browsers, which needed to address security vulnerabilities separately, started to warn users by labeling websites that used old SSL certificates as unsafe. These drawbacks give TLS many advantages. To switch to TLS, SSL 2.0 and SSL 3.0 must first be disabled in server settings.

Our assessment of local banks' SSL protocol support revealed that none of their websites were SSL supported.

4. TLS&SSL

4.4 RC4 support

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

The RC4 is no longer considered safe, and careful consideration should be given to its use. For websites, it allows part of the encrypted HTTPS traffic to be decrypted (such as the session ID transmitted in Cookies) in dozens of hours. It also makes it possible to implement a MitM attack, eavesdrop and save encrypted traffic, and perform a large number of requests on behalf of the victim.

Our assessment of local banks for RC4 cipher support revealed that none of them use RC4 cipher for encryption.

4. TLS&SSL

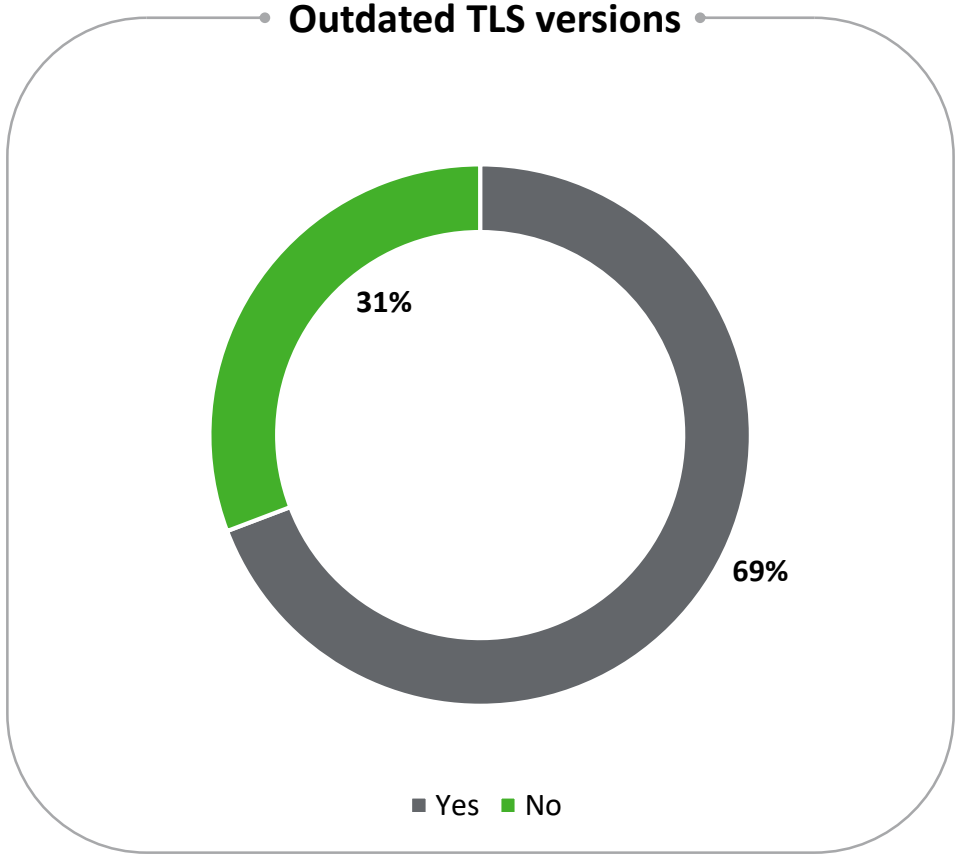
4.5

Outdated TLS versions

Transport Layer Security (TLS) provides encrypted communication for security and privacy. TLS 1.0 has been around since 1999, and it is an evolution of the older SSL encryption protocol. There is also the more modern TLS 1.2, which appeared in August 2008, and the most current TLS 1.3, which was released in August 2018.

A vulnerability in TLS 1.0 was discovered in 2011 that allows cookies used to authenticate users to be decrypted. Moreover, unreliable MD5 and SHA-1 hashing algorithms are used in TLS 1.0 and 1.1. In 2020, all major browsers disabled support for TLS 1.0 and TLS 1.1. Disabling these protocols is also recommended on the server side.

We found that 69% of Azerbaijani bank websites still support the vulnerable TLS versions 1.0 and 1.1. The remaining 31% support secured TLS protocol versions only.



4. TLS&SSL

4.6 SSL Renegotiation

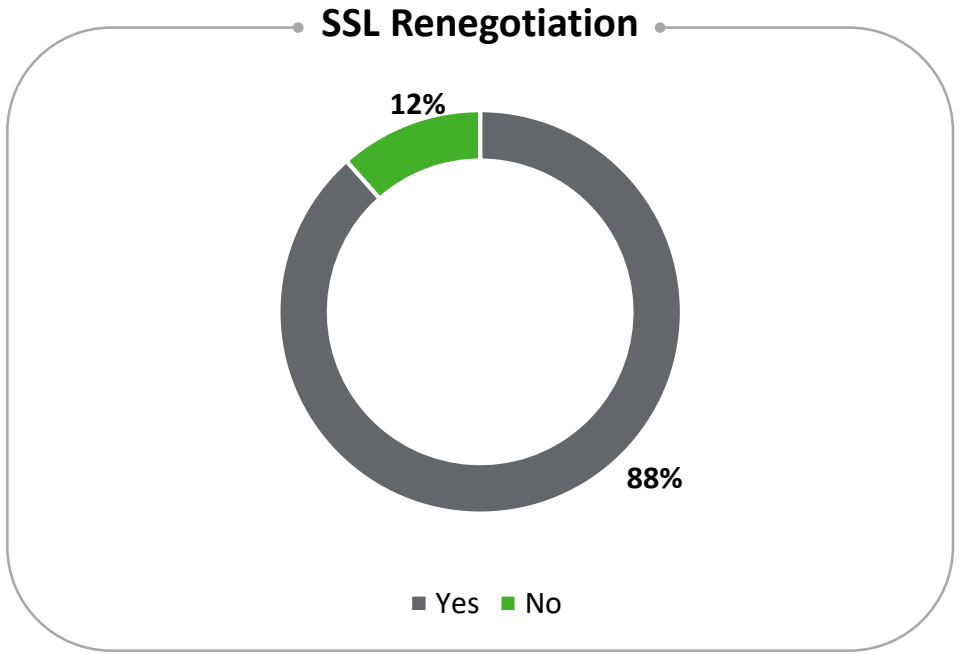
SSL renegotiation is useful when a regular SSL session has already been established and client authentication is required. For example, let's say you are browsing an online shopping site that uses SSL, which is HTTPS. Initially, you browse the site anonymously, adding items to your cart. But when you decide to make a purchase, you will be prompted to log in to the site, forcing you to set up an SSL connection to allow authentication. Any information collected prior to this authentication (for example, items added to the cart) should be preserved even after authentication. Thus, the newly established SSL session uses the existing connection. Note that renegotiation can be requested by either the client or the server at any time.

SSL Renegotiation can have known vulnerabilities if configured insecurely, which is why some developers prefer to disable SSL Renegotiation on the server side.

However, problems arise when servers disable renegotiation and provide no indication of their security status: some are secure while others are not, and browsers can do nothing without knowing this information. This inconveniences users and forces them to manually configure their protection levels.

For this reason, it is highly important that the server only allows secure renegotiation and limits the number of SSL handshakes, or refreshes the server's resources by adding products such as an SSL accelerator.

Our review of local banks' websites revealed that 12% of them have insecure or disabled SSL renegotiation, while the remaining 88% have secured renegotiation enabled.



4. TLS&SSL

4.7 Beast vulnerability

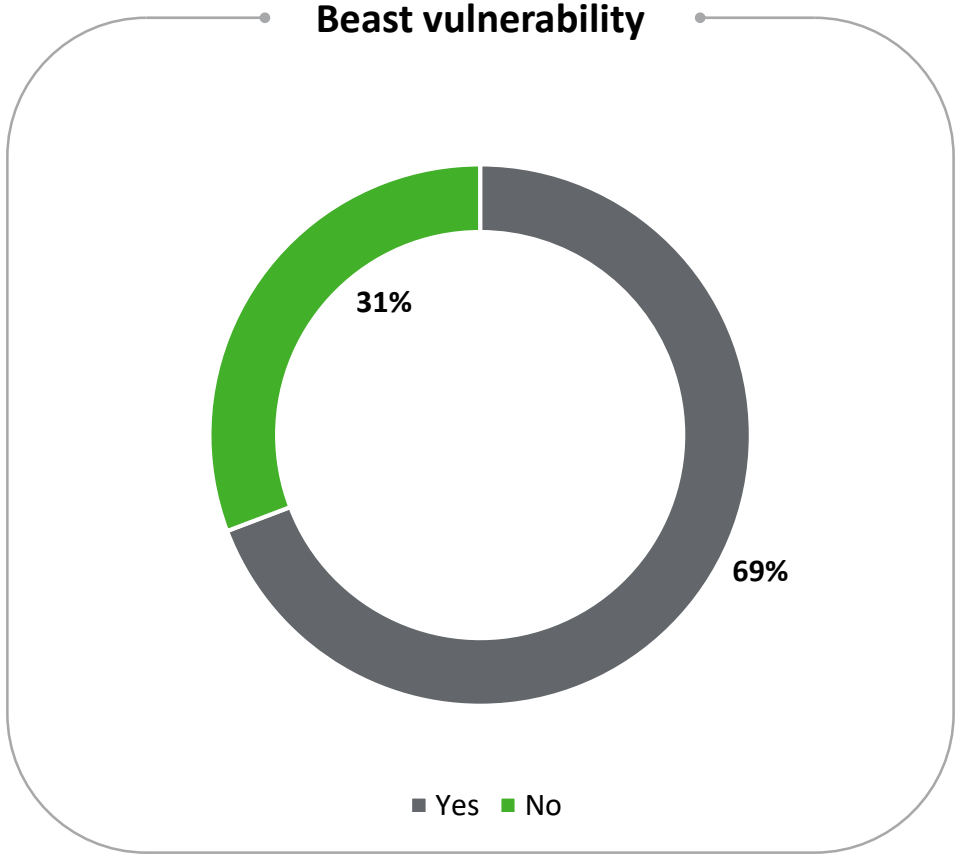
Pre-2006 versions of the affected TLS protocol are now vulnerable to Beast attacks. Attackers can decrypt data exchanged between two parties using TLS 1.0, SSL 3.0 and below. For this attack technique, the attacker and the victims must be in the same network (man-in-the-middle).

Thanks to the BEAST method, passwords can be divided into small packages and decrypted. Hackers who decrypt one byte of data in two seconds can gain access to credentials using an authentication system of 1000-2000 characters in half an hour. Some say that this time has even been reduced to 10 minutes. In this method, a Java applet is used to bypass the same-origin policy (SOP).

In 2011, security researchers discovered more practical ways of exploiting the Beast vulnerability. Data encrypted using the CBC mode with chained IVs allows MitM attacks to be performed in order to obtain plaintext HTTP headers via a blockwise chosen-boundary attack on an HTTPS session, together with JavaScript code that used the Beast attack.

The best way of protecting users from Beast attacks is to disable SSL and versions of TLS older than 1.2 on the server side.

Our assessment of local banks' websites revealed that 69% are potentially vulnerable to Beast attacks due to their support of old TLS versions, while the remaining 31% are not vulnerable.



4. TLS&SSL

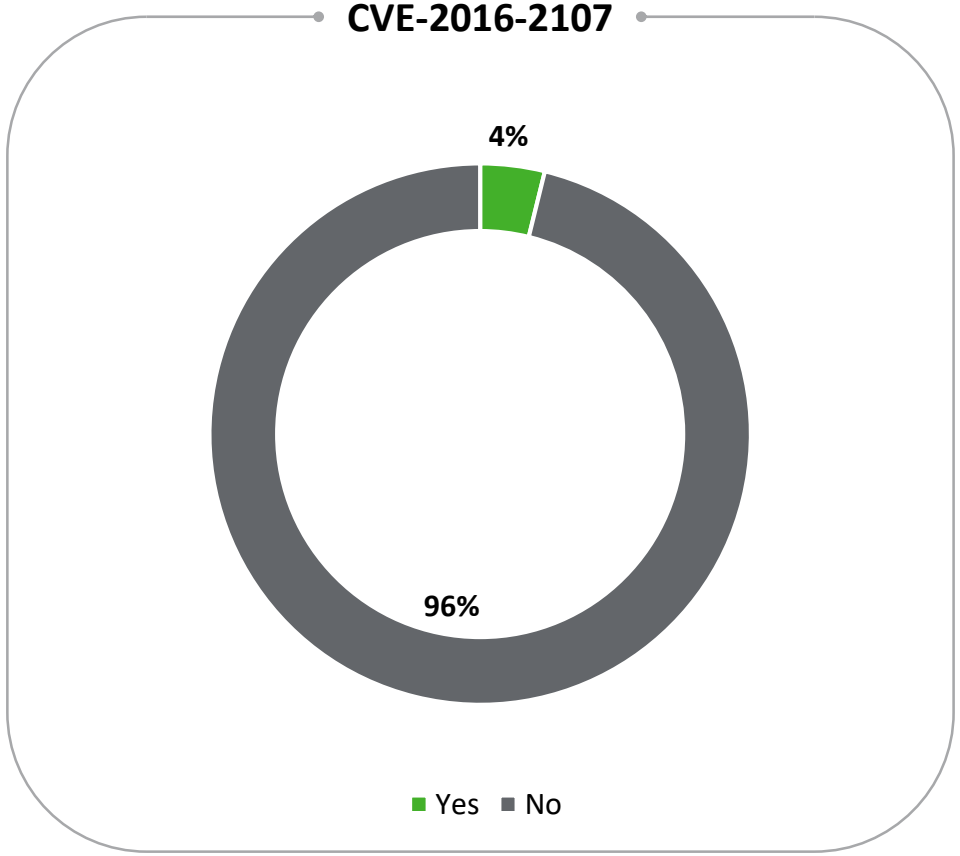
4.8

CVE-2016-2107 vulnerability

In the first half of 2016, most encrypted sites were threatened by the CVE-2016-2107 vulnerability, which became known in 2013 as a result of the fix for the Lucky 13 vulnerability. This vulnerability allows MitM attacks to be performed and sensitive information to be retrieved in the plaintext as a result of padding-oracle attacks against AES CBC sessions.

Although this vulnerability has been closed with a new patch for OpenSSL, some websites still use outdated OpenSSL versions.

Our assessment of local banks' websites revealed that 4% (one website) was vulnerable to CVE-2016-2107, while the remaining 96% had non-vulnerable versions of OpenSSL.



4. TLS&SSL

4.8

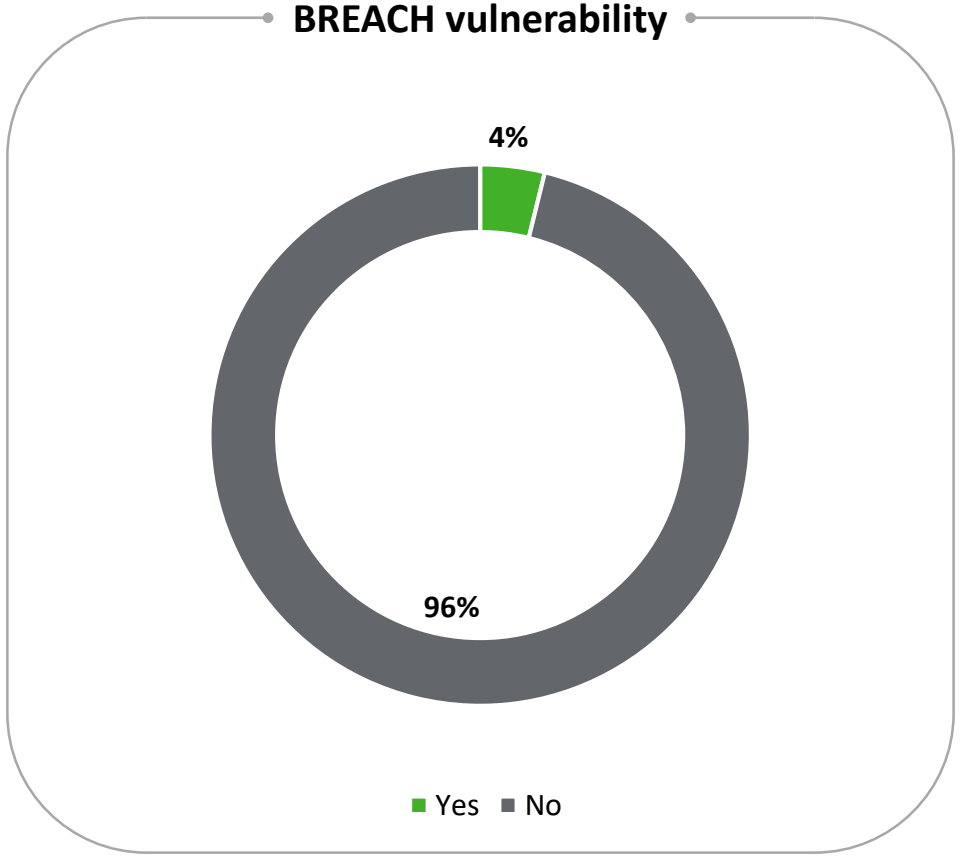
BREACH vulnerability

The BREACH vulnerability, or Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext, attacks HTTP responses by exploiting flaws in common HTTP compression. This attack was first introduced in 2013.

All sites that use SSL/TLS encryption with preliminary compression of traffic and the gzip/DEFLATE compression algorithm, and simultaneously allow the sending of user-modified requests of arbitrary content (such as search queries) to the site, are vulnerable to BREACH.

By exploiting the BREACH vulnerability, attackers are able to leverage information leaked by compression to recover targeted parts of the plaintext.

Our assessment of local banks' websites revealed that 4% (one website) was exposed to the BREACH vulnerability, while the remaining 96% were not vulnerable.

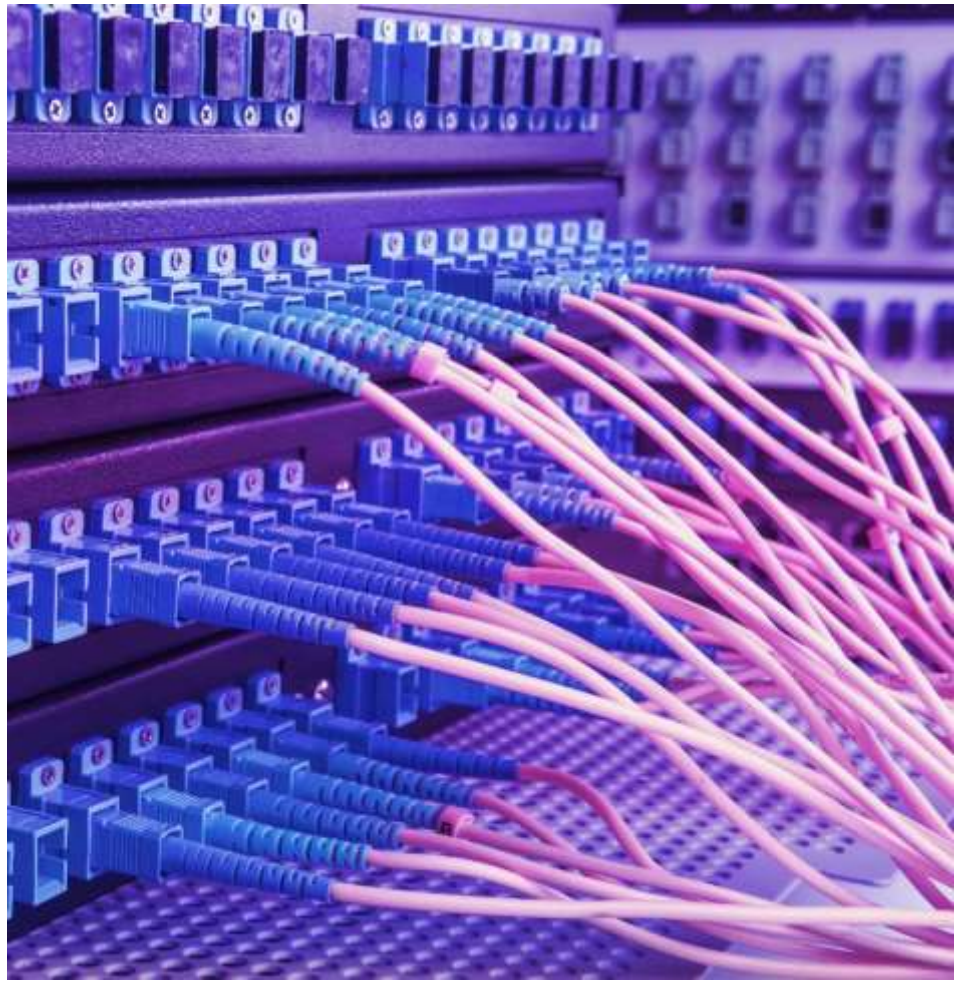


4. TLS&SSL

4.10

Other vulnerabilities

In addition to the above mentioned observations, we checked each target in the scope of this report for POODLE, FREAK, Logjam, DROWN, ROBOT, Heartbleed, and Ticketbleed vulnerabilities. We found that none of the websites of local banks were exposed to such attacks.



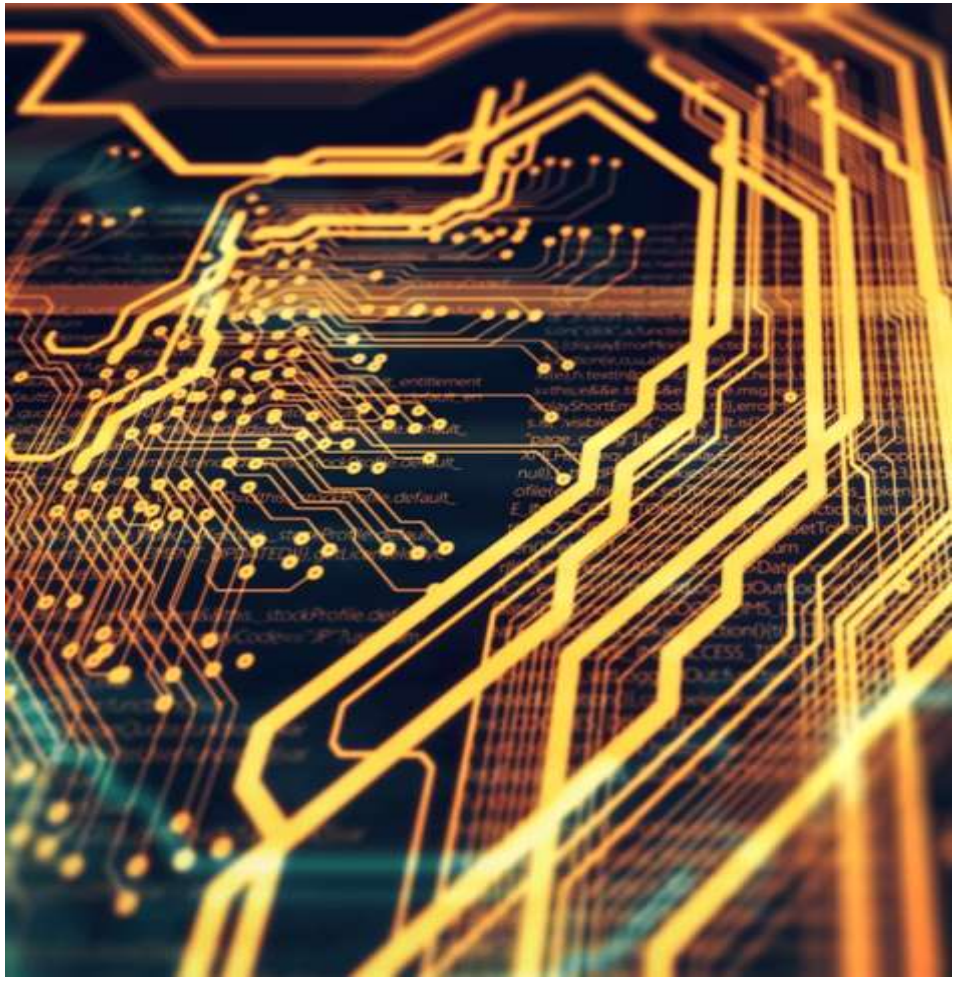
4. TLS&SSL

4.11

Conclusion

As we have seen, implementing TLS is vital to keeping the data of banks and their clients secure on the Internet. However, wrongly configured webservers may expose data rather than protect it.

Our assessment revealed that on the websites of Azerbaijani banks, SSL/TLS settings are more or less covered. Nevertheless, some banks still feature outdated protocol support, leaving them potentially vulnerable to related attacks.



Email leaks

1. Availability
2. Domain reputation
3. HTTP Headers
4. TLS and SSL
5. **Email leaks**
6. Open ports
7. Cybersquatting
8. GDPR Compliance

5. Email leaks

05

Data leaks happen quite often, which is one of the drawbacks of the digital world. Even when organizations protect their web resources and information assets responsibly, the human factor still puts them at risk. Employees without cyber awareness often use corporate emails to register with third-party web resources.

Because cyberspace is becoming more and more exposed to sophisticated cyber-attacks, even organizations that prioritize security are at risk of data breaches. The website *Information is Beautiful* has created an impressive visualization of data leakage statistics, available here. This statistical information demonstrates that many top-ranked organizations worldwide have experienced data breaches, which has allowed malicious people to create databases of usernames and passwords by collecting leaked information. Some try to grow these databases with information they obtain from each new leak and sell it wholesale on the black market.

Organizations must be prepared to handle situations when employee credentials are leaked following a data breach on a website where an employee had registered using their corporate email. Technically uninformed people may use the same or similar variations of credentials on several web applications, and the leaked password and the corporate email password may match or differ only slightly. Hacked corporate emails can then be used to retrieve sensitive information, conduct phishing attacks against privileged users, or share compromising data on behalf of the organization. This puts the organization at risk of losing finances, the trust of clients, and its reputation.

Resources exist to help organizations determine if any of their accounts have been compromised during a data breach. Anyone can use haveibeenpwned.com to find out whether a particular email has been leaked in a data breach; if this is the case, the website will provide the details. Users only need to type in the email address to which their accounts are linked to find out whether it appears on a one of the databases leaks compiled by haveibeenpwned.com.

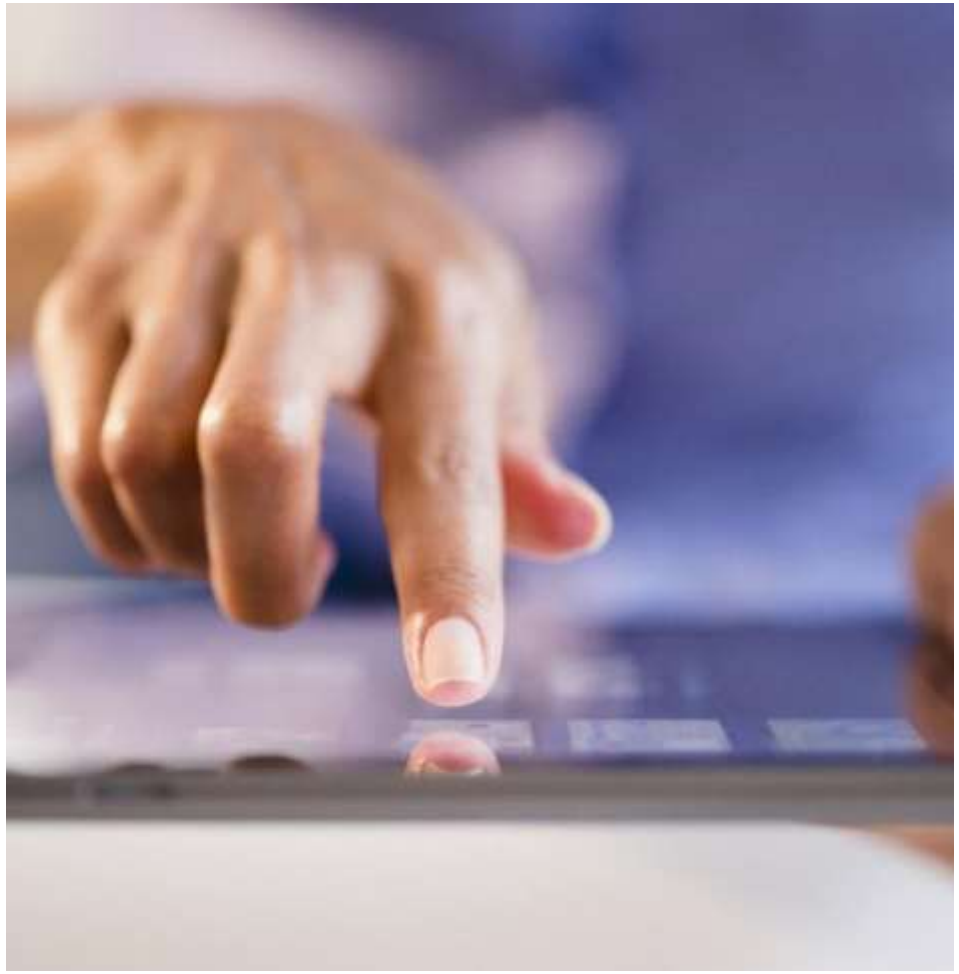
5. Email leaks

5.1 Our assessment approach

For the purposes of this report, we have compiled a list of employees of all local banks based on publicly available information from social networks (such as LinkedIn), after which we used an automated information gathering tool. Next, we determined the email compilation pattern of each bank using Hunter.io, which allowed us to construct a list of potential corporate emails addresses based on the first and last names of previously identified employees. We checked to see whether any of these emails had been leaked using Haveibeenpwned.

Each bank was placed in one of the following categories based on the numbers of corporate email addresses leaked to the Internet as a result of a third-party breach:

1. Less than five leaked email addresses
2. From six to 50 leaked email addresses
3. From 51 to 100 leaked email addresses
4. More than 100 leaked email addresses.

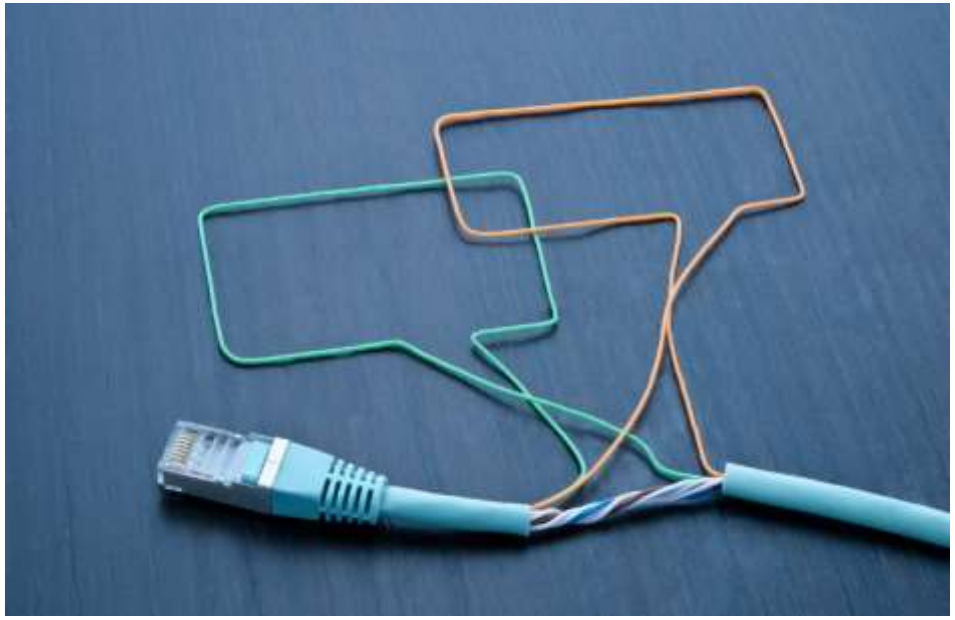


5. Email leaks

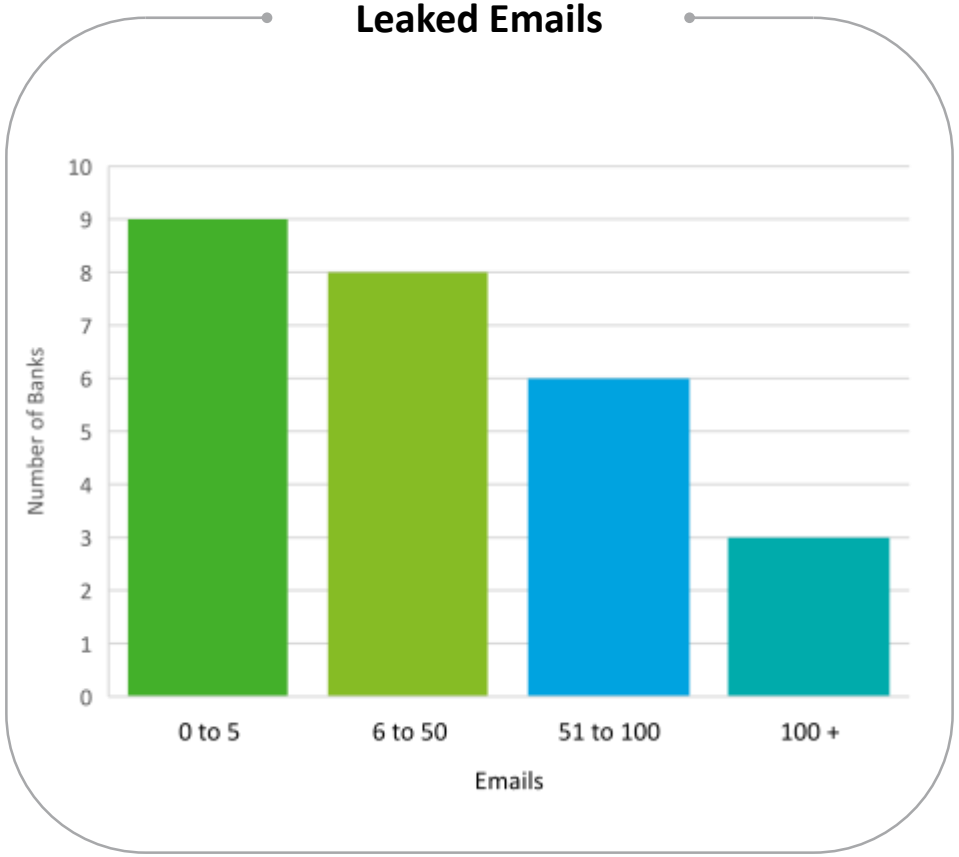
5.2

Results

Our assessment revealed that there were 26 local banks with 100+ email addresses leaked on the Internet. Six banks had between 51 and 100 leaked emails, while eight had between six and 50; the remaining nine banks had less than five corporate email addresses leaked.



Leaked Emails



5. Email leaks

5.3 Conclusion

To avoid information leaks, banks must take all risks into account and properly educate their employees by raising awareness of cybersecurity matters.

This work should take the form of a designated program provided on a regular basis.

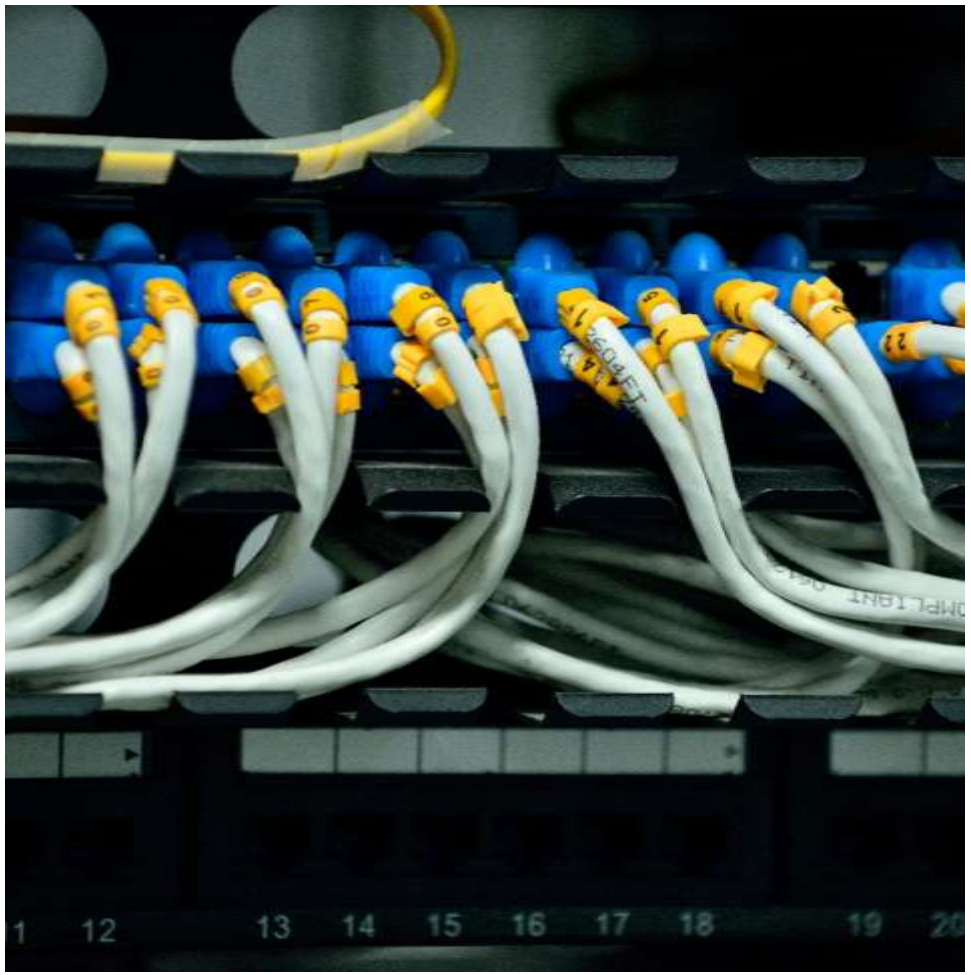
Security awareness programs should comprise the following activities:

1. Phishing tests: to assess the current level of awareness among employees and identify risk areas;

2. Interactive workshops: to raise awareness on information security;

3. E-learnings: to educate and evaluate personnel within different subject areas, ensuring they have the required cybersecurity competences;

4. Activities to sustain a culture of security: to follow-up on the cyber security landscape and threats and keep the program up-to-date.



Open ports

6. Open ports

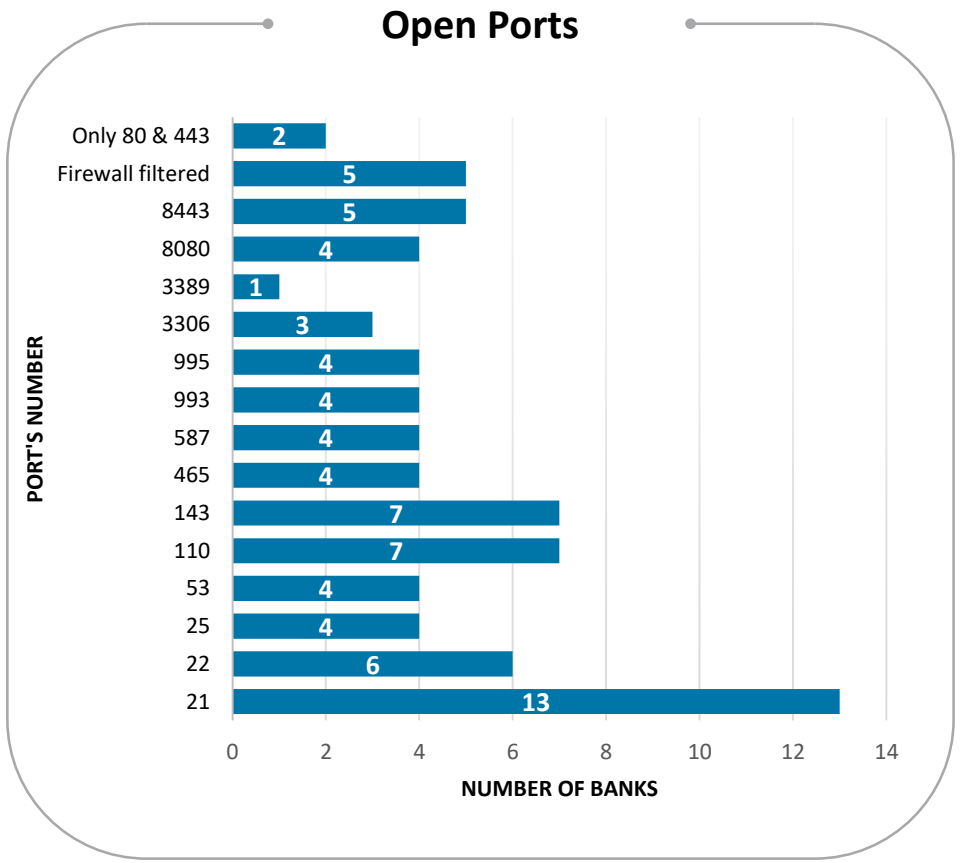
06

We analyzed externally accessible ports that are not necessary for the functioning of a website. Although the presence of unnecessary open ports is not necessarily a sign of vulnerability, good practice maintains that ports and services that are not mandatory for a website's operation should be either closed or filtered using a security appliance or software. Websites require ports 80 (HTTP) and 443 (HTTPS) to function and be accessible to the public.

To identify the state of ports, we used the Nmap scanner tool with non-intrusive scanning options. For the purposes of this report, we only analyzed the top 100 most common ports.

Our tests of open ports on the web servers of local banks showed that out of 26 test objects, two had only necessary port open, five filtered ports using security solutions, and the remaining 19 webservers had open ports other than 80 and 443.

We have presented statistics for each port in the chart below.



6. Open ports

6.1 Conclusion

Increasing webserver security by reducing attack vectors should be a key objective for administrators. This can be achieved by installing and maintaining only absolutely necessary services (ports) that give access to internal and external customers.

That said, some admins are overzealous with this principle and allow port 443 on their webservers while blocking port 80. However, allowing port 80 does not increase the attack surface on webservers, as such requests are generally served by the same software that runs on port 443.

Cybersquatting

7. Cybersquatting

07

Cybersquatting is the registration of domains that are consonant with the names of well-known brands for the purposes of subsequent resale, phishing attacks, or illegal use to offer competing goods and services. Sites registered by cybersquatters can mislead existing users, thereby damaging the reputation of bona fide organizations.

Many forms of cybersquatting can harm banks. The creation of a website with a similar name to a real website, containing announcements or news to be published on behalf of the bank, may leave banks and their brands in a very difficult situation, especially if data on the fake website, such as contact information, is real. To protect themselves from such risks, organizations must analyze this attack method thoroughly and practice defensive cybersquatting.

Defensive cybersquatting means becoming the legal owner of numerous domains that sound like the original trademark. Taking this measure makes it possible to redirect potential visitors to the main domain and protect copyright holders from the unauthorized actions of other cybersquatters.

For this assessment, we analyzed the defensive cybersquatting practices of all 26 local banks in our scope. The checklist contains domain names constructed from homoglyphs and double-letter variations.

Homoglyphs are signs that are graphically identical or similar but have different meanings, such as the letter “O” and the number “0.” Homoglyphs can also result from using different alphabets. We used the following table during our check:

l	**1**
o	**0**
l	**j**
m	**rn**
q	**g**
d	**b**

For example, using the table above, we constructed the following domain names from “randomsite.az”:

rand0msite.az

randornsite.az

randomsjte.az

Doubling letters in domain names is another effective cybersquatting technique. Thus, the domain name randomsite.az could be changed to something like randomsiite.az, which is an inconspicuous alteration that could easily escape users’ notice unless they are paying close attention.

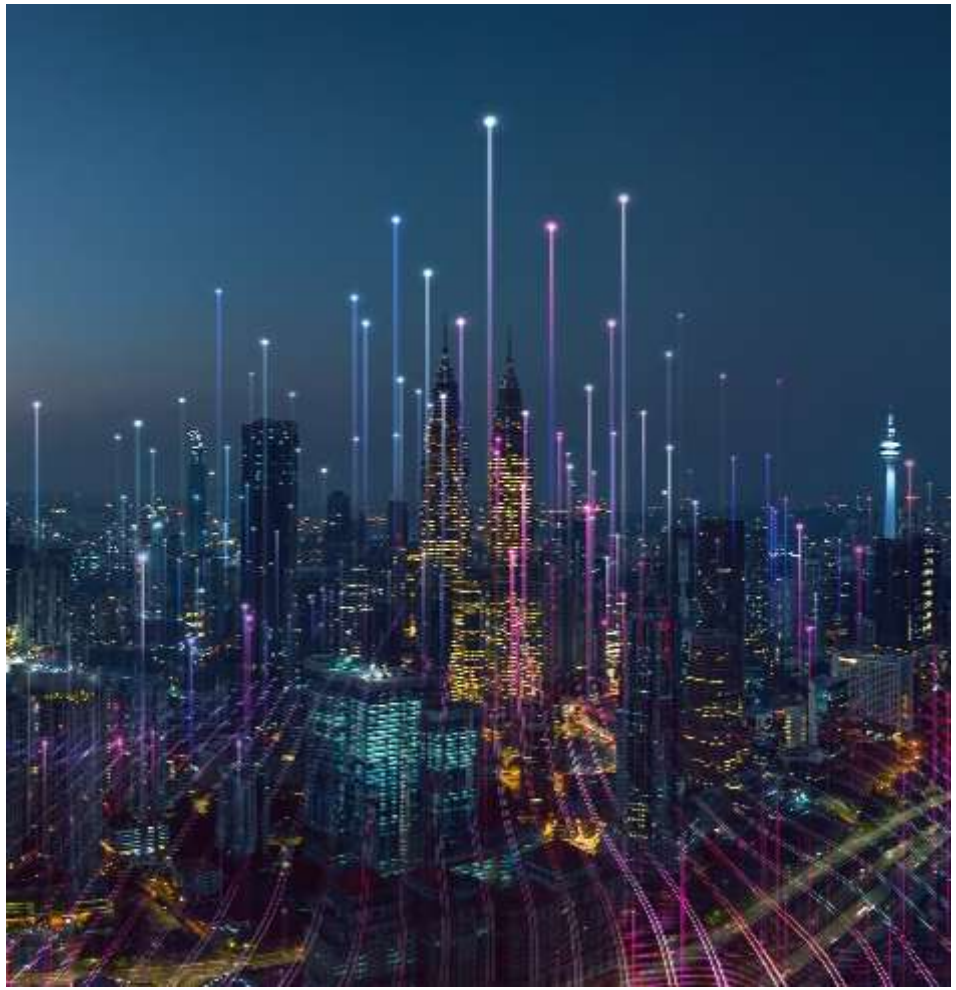
Our assessment revealed that no Azerbaijani banks in our scope practiced defensive cybersquatting by registering homoglyph and double-letter variations of their domain names.

7. Cybersquatting

7.1 Conclusion

Cybersquatting has become a lucrative online practice that can have a negative impact on the reputation of well-established commercial brands. The owners of such brands or trademarks may face legal challenges when attempting to tackle cybersquatting issues, as it can be difficult to ascertain whether such practices are legal or illegal, because the phenomenon combines both legitimate and illegal activities.

Although domain name disputes that arise from cybersquatting and related practices can be resolved through Uniform Domain Name Resolution Policy procedures, preventive measures allow owners to save money on the fees required to initiate this process. Trademark owners can register domain names that are confusingly similar to their trademark, thereby preventing cybersquatters from registering them first. However, our analysis shows that this practice is not common among local banks, nor is it part of their cyber security strategy. This can lead to a wide range of unmitigated cyber risks.



GDPR Compliance

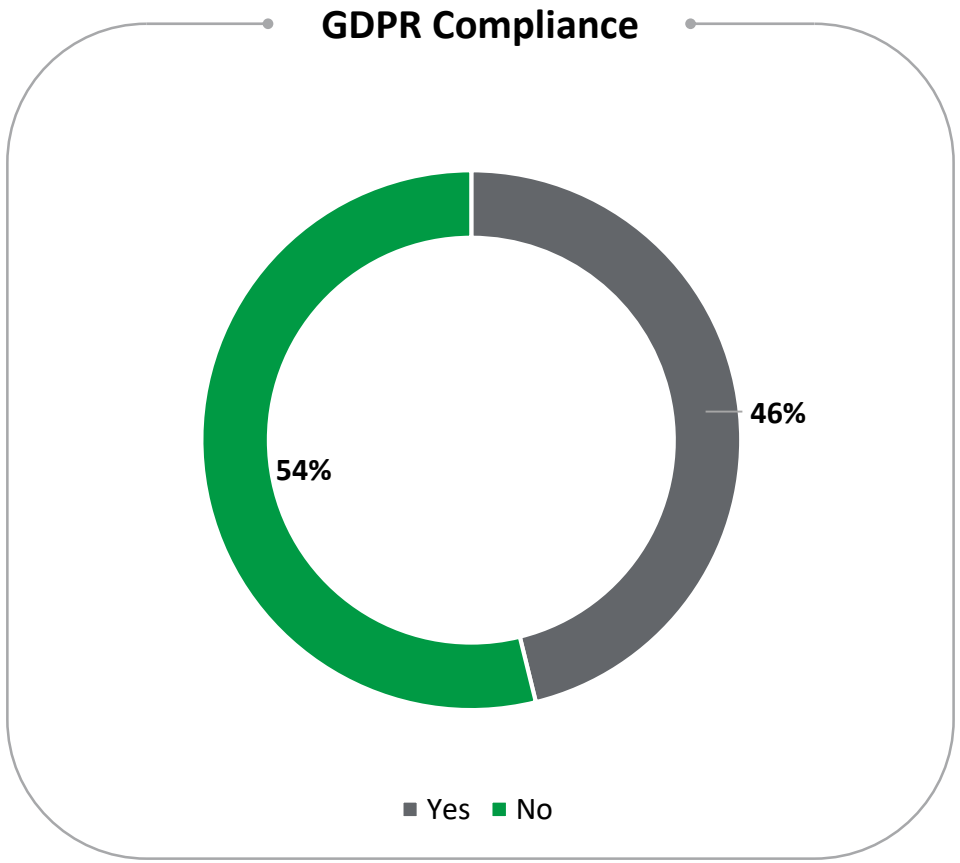
8. GDPR Compliance

08

GDPR, or the General Data Protection Regulation, is an EU regulation on data and privacy protection that covers all individuals located within the European Union. The GDPR is concerned with any works and services that involve collecting the personal data of people living in the EU.

According to the European Commission, personal data includes any information about a person, whether or not it is related to his or her private, professional or public life, such as names, home addresses, photos, email addresses, banking information, social media posts, medical information, or IP addresses. This means that websites should not collect statistics and personal information or store unnecessary cookies for sites' technical operation without the prior consent of the user.

Our review of banks' websites revealed that only 46% were aligned with GDPR requirements, while the remaining 54% violated certain requirements.



8. GDPR Compliance

08

Conclusion

The legislation of the Republic of Azerbaijan does not oblige legal entities that provide financial services to comply with GDPR requirements. However, Paragraph 2 of Article 3 of the GDPR, which covers territorial scope, states that even companies established outside the EU are subject to GDPR requirements if they offer goods or services to real persons (data subjects) living in the EU or monitor the behavior of such persons, irrespective of whether a payment is required from the data subject. In other words, if any bank is storing the data of at least one customer from Europe, it automatically falls under the GDPR. Moreover, compliance with GDRP requirements may be a decisive factor for prospective organizations (especially from the EU) that are looking for a partner for financial services.

Deloitte.