Kaspersky Fraud Prevention

Fraud report based on Kaspersky Fraud Prevention data

kaspersky BRING ON THE FUTURE

More information at kfp.kaspersky.com

Contents

General statistics based on Kaspersky Fraud Prevention data

The Kaspersky Fraud Prevention report is based on incidents associated with cybercrime and on data detected by Kaspersky Fraud Prevention after thorough analysis of consumer behavior in the system.

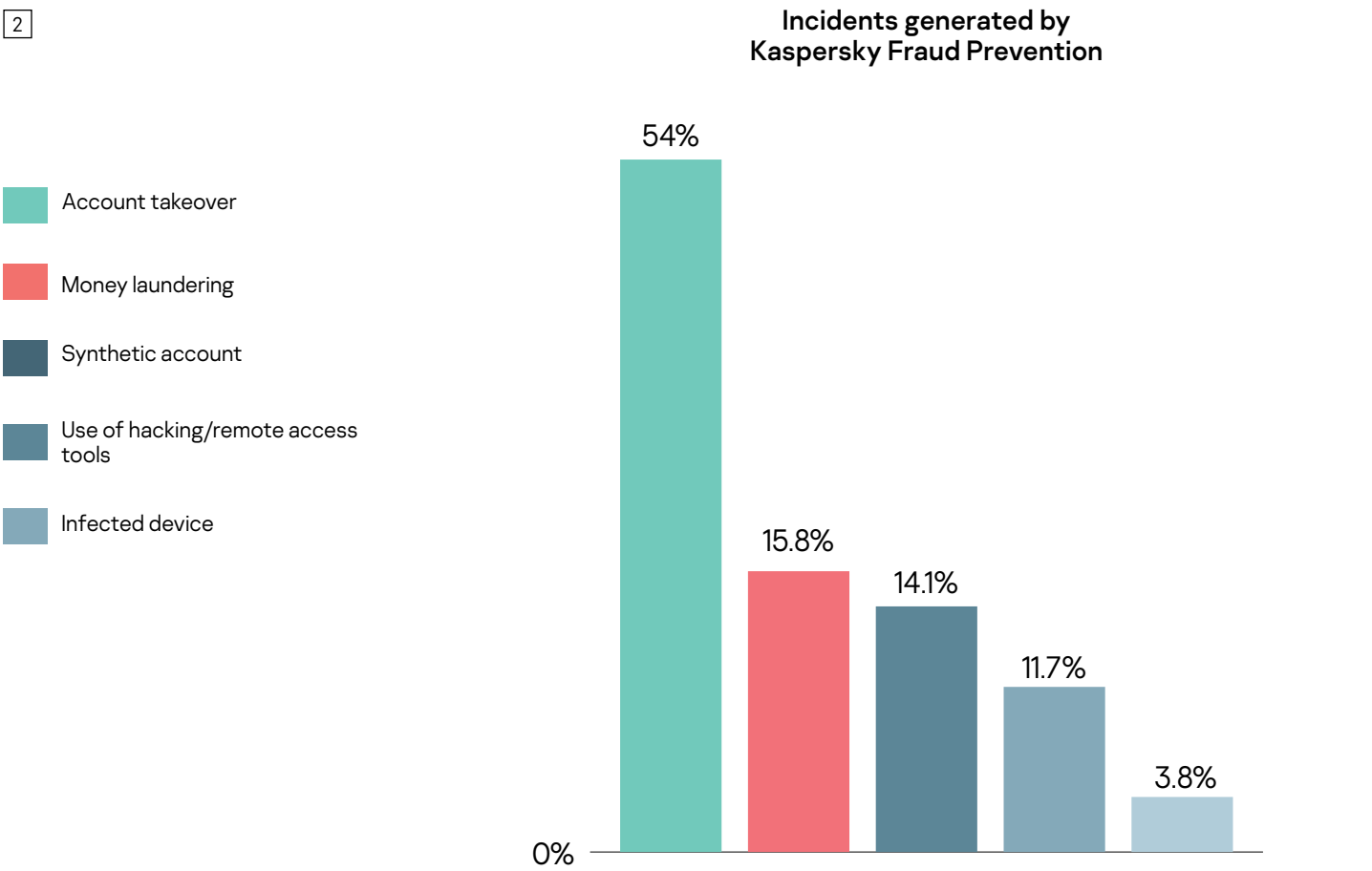
In this report, we discuss the main threats encountered by companies, analyze current cyberfraud trends with a focus on cybersecurity issues in the banking sector and e-commerce, as well as present our main conclusions.

1

Kaspersky Fraud Prevention processes traffic in real time according to the following parameters:

Metric name	Number of unique units per day
User	502,167
Device	729,936
Online session	935,143
Processed events	19,838,373

2



Session events analysis with Kaspersky Fraud Prevention

Device and environment analysis

Leverages the global presence of Kaspersky to identify "good" devices and use this knowledge for user authentication. Based on global device reputation, IP address, location parameters and more, any attribute previously linked to fraudulent activity is proactively detected and marked as suspicious or related to fraud.

Behavioral analysis

Tracks user activity during login and throughout the session, analyzing typical navigation, time patterns, account activity and clicks, etc. This data allows profiles of normal behavior to be built and any abnormal or suspicious activity to be detected during the login stage.

Behavioral biometrics

Analyzes unique user interaction with the device, like mouse movements, clicks, touches, swipe speed and more to detect whether a device is being used by a legitimate user or an intruder, a human or a machine. This technology can also be used to detect bots, remote administration tools and account takeover.

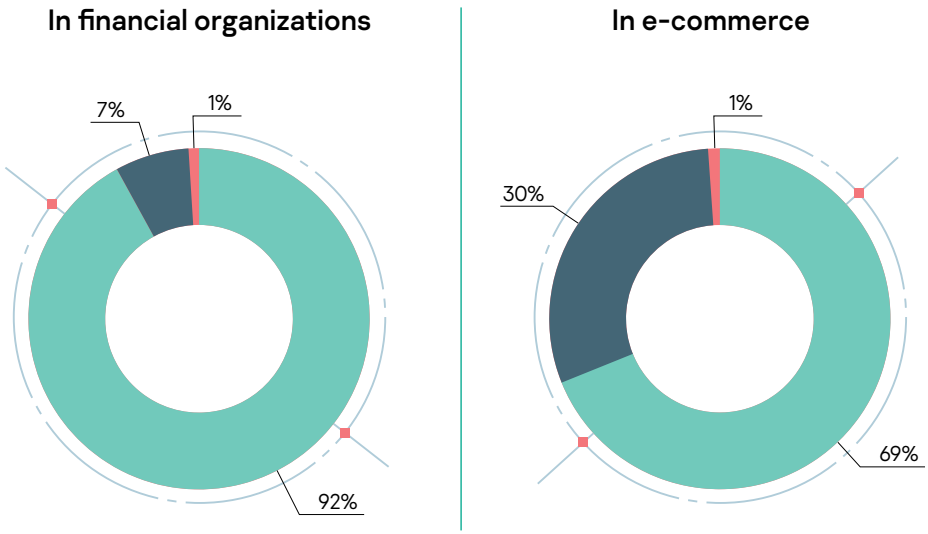
Malware detection

Can determine whether a user device is infected with malware without the installation of additional components. Data on possible infection is used for risk-based authentication (RBA) as well as for determining the legitimacy of transactions.

3

Risk-Based Authentication eliminates the need for additional authentication steps for legitimate users, allowing them to log in without excessive verification. By constantly analyzing hundreds of different indicators in real time, a dynamic assessment of the level of risk is formed. It allows a decision to be made with a high degree of confidence regarding the level of access to a personal account.

Annual average ratio of online user session risk-level verdicts



Cyberfraud trends

YouTube can be cited as proof of the increase in user traffic: the company was forced to reduce the load on its servers by reducing video quality.

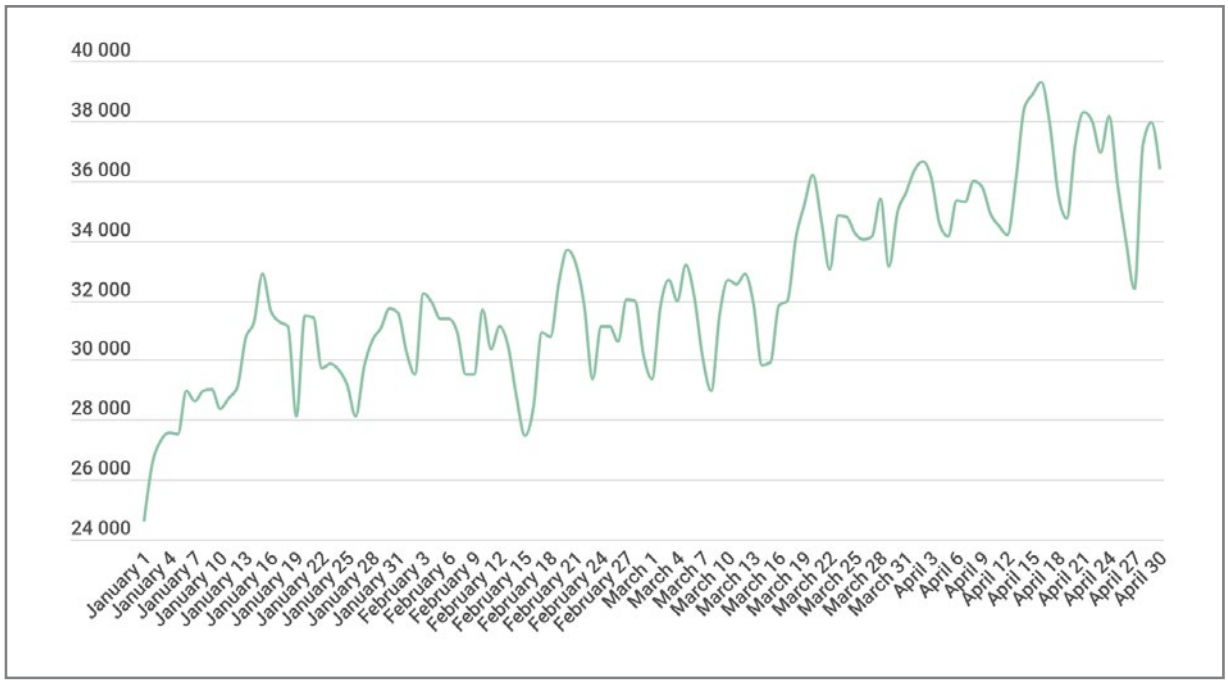
Cyberfraud during quarantine

In 2020, the COVID-19 pandemic changed the way most people live. And some people even benefited from this situation, such as online fraudsters. We won't assert that the increase in fraudulent activity is entirely due to the pandemic, but there are some reasons for this assumption.

A lot more people are spending a considerable amount of time online, and the amount of time people spend online in general has also increased. For phishers and spammers this means only one thing: more potential victims.

Kaspersky's antivirus team recorded a 25% increase in the average daily number of web antivirus triggers for Kaspersky customers since the beginning of 2020.

4



Number of web antivirus detections, January - April 2020

Fraudulent sites, such as phishing sites, sites with active push notifications, or sites with "scare messages" about operating system malfunctions and errors, were among the many reasons for antivirus triggers in cases where resources redirected users to those sites.

Other reasons for the growth of cybersecurity incidents include: the spread of modifications to Trojan-PSW browser scripts, web resources with adware scripts and pages that perform cookie stuffing.[1]

[1] More information is available at https://securelist.com/cyberthreats-on-lockdown/96988/

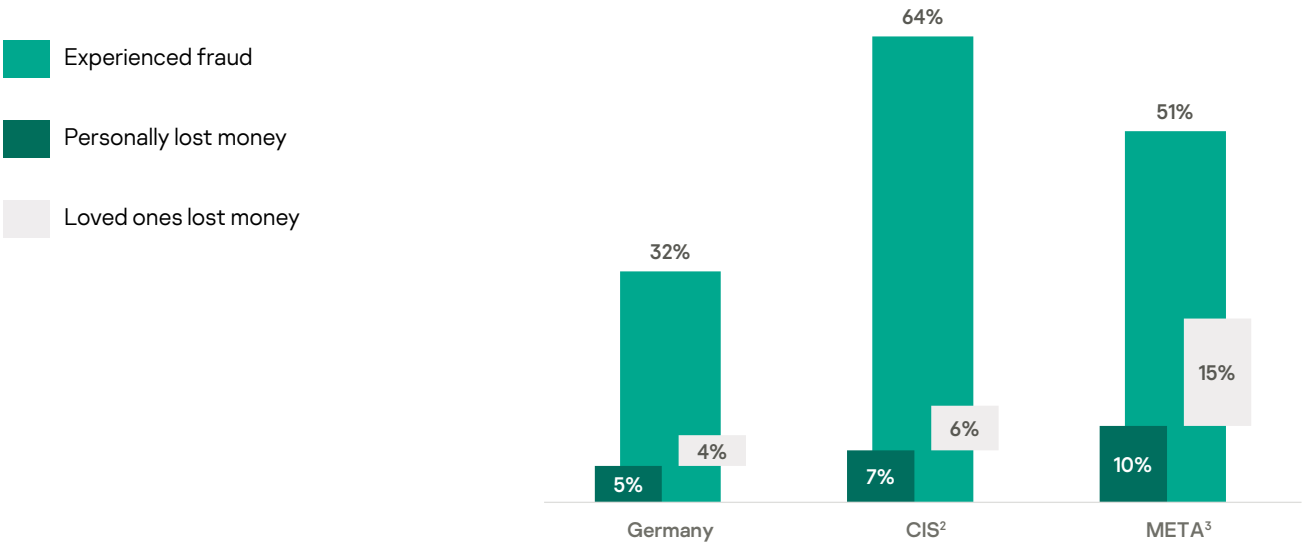
Social engineering

Kaspersky conducted a study into telefraud, which includes phone calls, text messages and emails.

The main difference between those who have encountered fraud and those who have not is the **level of income and confidence** in their knowledge of modern technology:

- People who have encountered fraud **usually have above-average incomes, believe they are well-versed in technology,** and make active use of various IT solutions to avoid fraud.
- Those who have not encountered fraud simply ignore **unknown numbers and don't open suspicious links.**

5



The results of the study revealed the following:

- Online fraud is more prevalent in developing countries (the CIS, Middle East and Africa) than in developed countries (Germany was chosen as the subject of the study). (See Fig. 5.)
- More often than not, people with lower-than-average incomes fall for telefraud. (see Fig. 8)
- About 20-30% of users use specific software solutions to protect themselves. These are typically users who are well-versed in modern technology. (See Fig. 7.)
- The most effective telefraud scheme is the creation of fictitious online stores using direct payments by card or phone number.
- One of the most popular methods is spam or text messages with eye-catching subjects like "you won" or "congratulations".

6

User protection measures. Before and after encountering fraud:

	Have not encountered fraud	Encountered fraud, but no money lost	Lost money due to fraud
Use a different password for important resources	82%	84%	78%
Read user agreement	69%	70%	72%
Use different browsers for different tasks	51%	53%	61%
Use different emails for different services	49%	54%	59%
Use different SIM cards or devices	32%	38%	50%
Use VPN/anonymizer services	23%	28%	44%
Provide inaccurate information	18%	30%	43%

[2] Russia, Kazakhstan, Belarus

[3] Turkey, UAE, Saudi Arabia, South Africa, Egypt, Bahrain, Kuwait, Oman

7

Change of behavior after encountering fraud:

	Have not encountered fraud	Encountered fraud, but no money lost	Lost money due to fraud
Do nothing	17%	24%	12%
Do not answer unknown numbers	61%	50%	64%
Use built-in features, e.g., black lists	22%	29%	39%
Use special programs	23%	20%	25%

8

Who encounters telefraud more often:

	Have not encountered fraud	Encountered fraud, but no money lost	Lost money due to fraud
Average age	39.0	37.3	36.6
Ratio of men to women	57:43	51:49	53:47
Can't afford large household appliances without a loan	49%	50%	**57%**
Think they know about technology	36%	47%	**49%**

Very often bank customers fall for the scam, believing they are getting a call from a bank employee to report a withdrawal or an attempted account hack, or to offer help in reducing card maintenance costs. Below is an example recorded by Kaspersky Fraud Prevention:

A client received a call from an unknown number. The caller introduced himself as a security officer at a large bank and reported that a large sum of money had been debited from the client's account. When the client states that their account at that bank doesn't contain that much money, the caller asked where the potential victim has such funds. The client named another bank. The client was then told to expect a call from the other bank.

A little later the client received a call from the number of the other bank. The client suspected possible fraud, opened the bank's website and checked the phone number, but when they saw that the call really was from the bank's official number, any suspicions disappeared. The client was told that an attempt was made to withdraw a sum of money from their account, and to return the money they need to provide the card number and the SMS code sent to confirm the operation.

The client gave the SMS code and card number and was also asked for the credentials to log in to the online banking service. The client provided the login and password.

After obtaining the data, the scammer withdrew a large sum from the client's account on the same day and also applied for a loan. The client confirmed that he did not make those transactions.

In the above case, the bank client provided all the necessary data to log in to their account, and the scammer subsequently logged in from their own device.

Another fraudulent technique – the use of applications with remote access tools – remains one of the most common. Fraudsters prefer applications such as AnyDesk, TeamViewer, AirDroid and AhMyth to remotely control user devices with Android versions 7.1-10.0.

Most often, the scammers introduce themselves as employees of the largest bank in the potential victim's region.

In this case, the scammers got the victim's bank wrong, but the fact that they used spoofed IP/SIP numbers "saved" them and managed to keep the victim interested.

Scammers have mastered the technique of substituting numbers for incoming calls. They often replace only part of their numbers with digits from a bank's number or display vanity numbers.

Unfortunately, banking institutions have accustomed their clients to being called from various numbers and callers introducing themselves as employees.

Here's information about some of the fraud attack scenarios we covered last year:

1. "The rescuer". Scammers who pretend to be security experts and act out scenariosto "save" users are called rescuers. They call bank customers posing as security officers and report suspicious charges or payments and offer their help. To provide help, the rescuer may ask customers to verify their identity through a code sent in a text message or push-notification to stop a suspicious transaction or to transfer money to a "secure account".
2. "The investor" The investor scenario involves fraudsters posing as employees of an investment company or investment consultants from a bank. They call customers offering a quick way to make money by investing in cryptocurrency or shares directly from the client's account, without having to go to a bank branch. As a prerequisite for providing the "investment service", the investor, like the rescuer, asks the potential victim for the code received in a text message or push notification. The tools are the same: IVR, RAT, SIP. The only difference is the source of the client database. The investor scenario is used if the potential victim has previously taken an interest in boosting their savings.

The scammer needs the victim to install a remote access application on their device. Once the user has installed the app on their mobile device, the cybercriminal gains access to all the features of the user's account. The scammer can transfer and withdraw funds, change account information, steal personal information to sell later, apply for loans, and more.

Based on the results of a joint study with Raiffeisenbank, employees of Kaspersky formulated several possible scenarios for such attacks:

1. The user is asked to state the approximate account balance and a one-time password, or to communicate them in some other way (for example, by entering them in touch-tone mode). After getting the necessary information, the attackers can withdraw funds from the account or take possession of the account data.

2. The intruder reports that a suspicious operation was prevented, asks the user not to report anything, but strongly recommends installing protection on their device. To do so, the user is prompted to download a program from a link sent in a text message and to install it on the device. If the user follows these "recommendations", a remote access program or malware (for example, ransomware that demands a fee to decrypt files or a banking Trojan) will be downloaded to their phone. Another variant involves the user being asked to go to an app store and download specific software found under "remote assistance" – most likely, this will also be a program for remote control of the device.

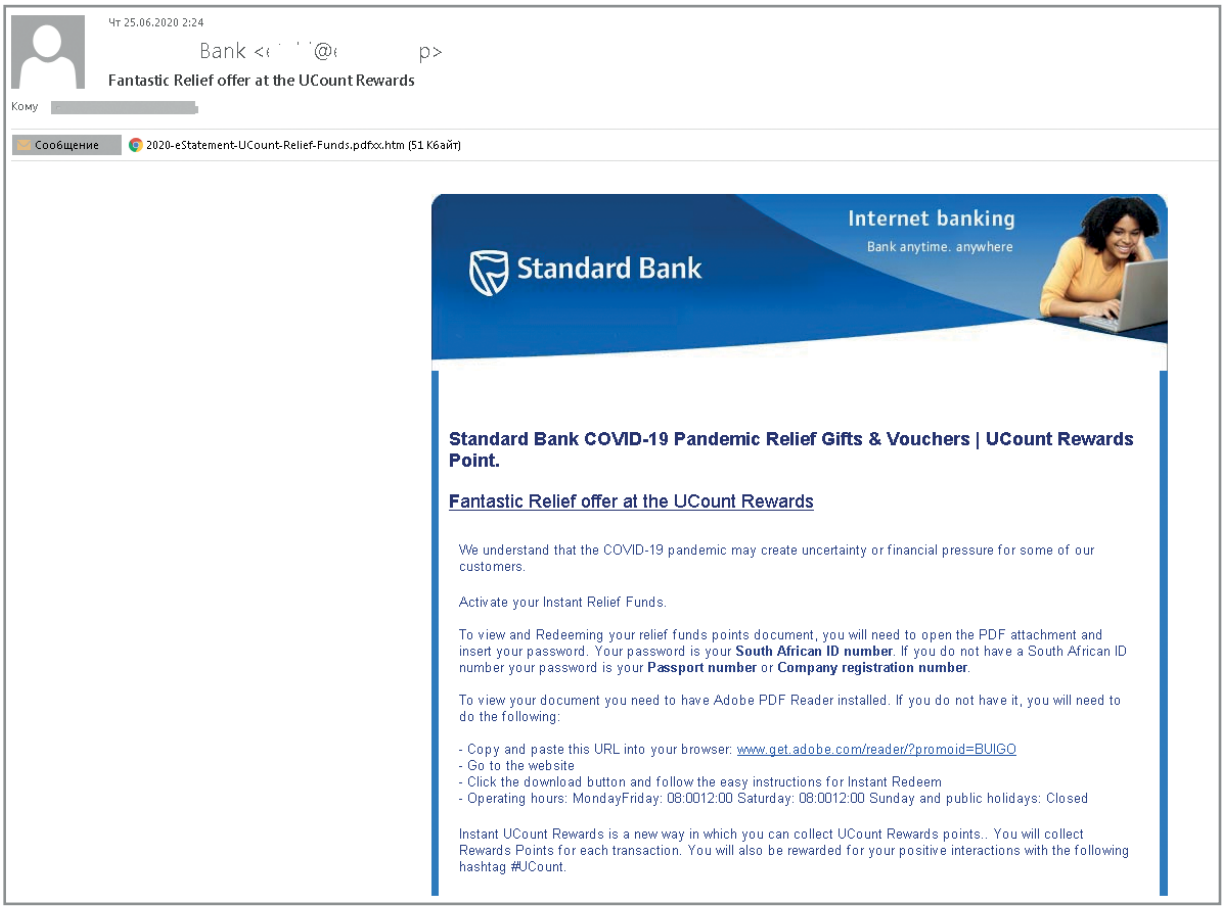
3. The scammer asks the user to install a certain program from the app store (Google Play Market or AppStore) by entering the word "support" or something very similar into the search field. At the top of the search results will be legitimate remote connectivity apps with ratings and number of installations, which plays into the hands of the attackers because it elicits a positive response from users. Once installed, the scammer asks the user to launch the banking app and turn their phone so the screen is facing down, because a transfer to a "secure account" will be made. This is when the criminal transfers money to a controlled account.[4]

[4] You can read more about the study at (Russian only) https://www.raiffeisen.ru/common/img/uploaded/files/news/card_fraud_trends2019.pdf

Bank phishing attacks amid the pandemic

Bank phishing attacks in the second quarter of 2020 were often carried out with emails offering various pandemic perks and bonuses to customers of banking organizations. To receive help, you had to download a file with instructions or follow a link. As a result, depending on the method used, the fraudsters can gain access to the user's computer, personal data or authentication data for various services. Below is an example of such a letter:

9



The COVID-19 theme also featured in the well-known method of fake letters from banks, which state that the customer's account has been blocked and in order to unblock it they need to enter their username and password on a special page.[5]

Gaining trust with the help of IVR (interactive voice response)

Another tool that seems harmless but is in fact readily exploited by scammers is the creation of an IVR menu for obtaining the second authentication factor. Attackers carefully select vocabulary and use a robot voice to make the request for the second factor sound as convincing as possible and to avoid raising suspicions in the victim. Users often perceive interaction with a robot as safer than human interaction. Prerecorded voice messages ask the victim to enter a code received in a text message or push notification. As soon as the victim tone-dials the code, the information is transmitted to the scammers' servers, and they immediately transfer the funds to the accounts they control, as the second factor is time-sensitive.

In 2020, scammers used the YouTube platform to attract victims to phishing sites.

The goal was to lure the potential victim to the fake site by telling them about the refund of a non-existent value-added or sales tax.

The video itself consisted of clips of news channels and instructions on how to "recover the money that was already paid".

After the victim went to the site, the payments were calculated and a conversation with a "bot-lawyer" took place, after which there was a request to transfer a payment for the services of the "lawyer".

[5] You can find out more at https://securelist.com/spam-and-phishing-in-q2-2020/97655/

Spam and phishing in 2020

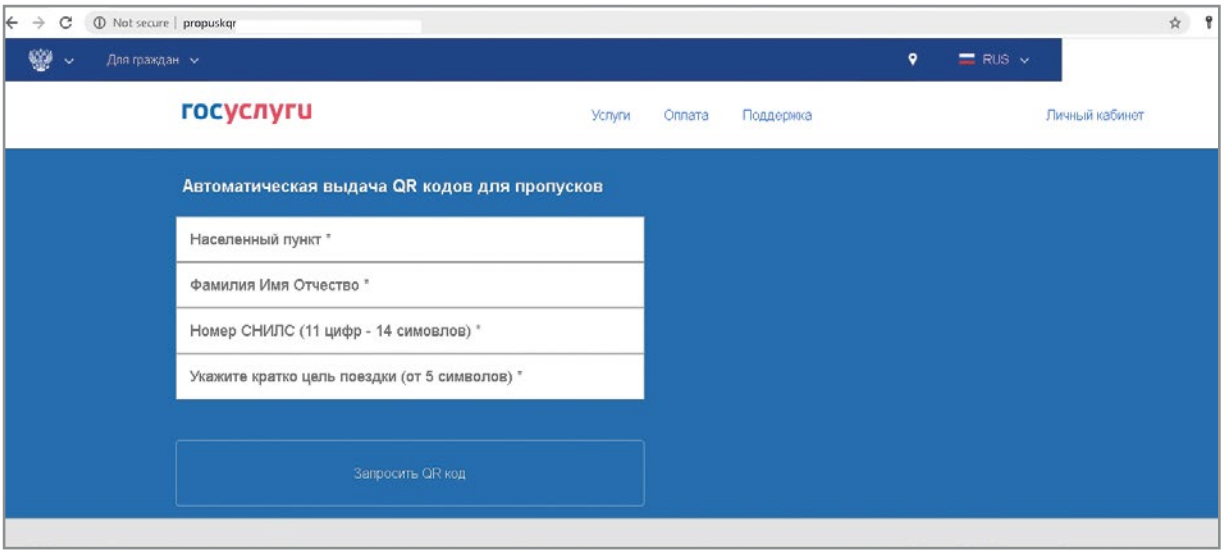
Fraudsters in self-isolation mode

Attackers responded to the self-isolation rules by creating a phishing site to collect users' personal data.

In order to obtain a pass to leave home, visitors to the site had to give their passport number, the purpose of their trip and send an SMS to a short number.

The fake site only bore a passing resemblance to the official portal.

10



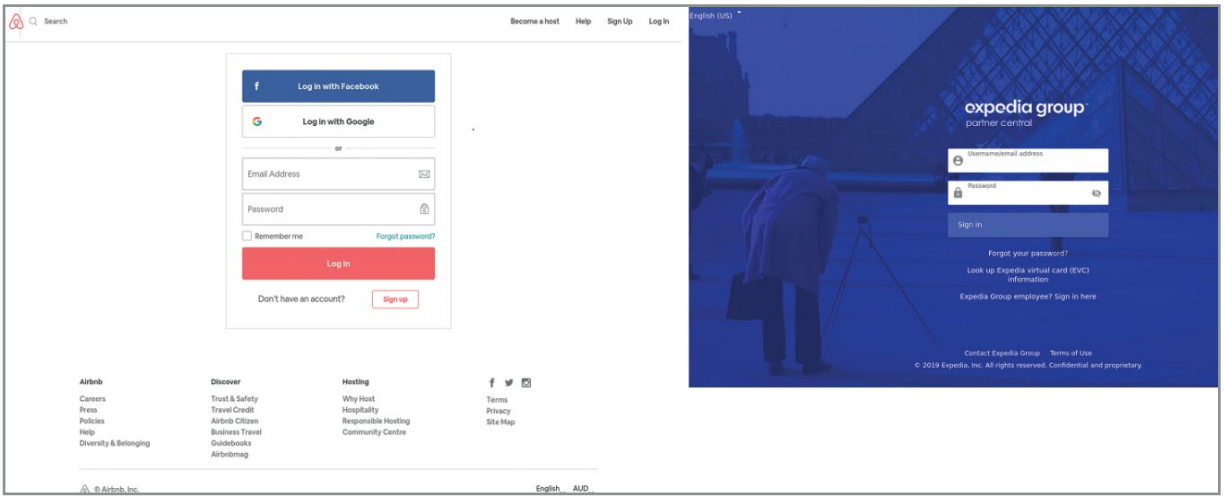
As a result of these actions, a sum of money was deducted from users' mobile accounts, their personal data ended up in the attackers' database and, of course, their passes remained unregistered.

In addition, the attackers offered ready-made passes for daily trips to work. Of course, there were no guarantees that the holder would not be fined for having a fake document during an inspection.[6]

Tourist phishing

These fake sites very accurately reproduced the design of the original travel company sites, and they can only be distinguished by closely examining the address bar: the most common telltale signs are the use of domains or free hosting addresses completely unrelated to the company in question.

11



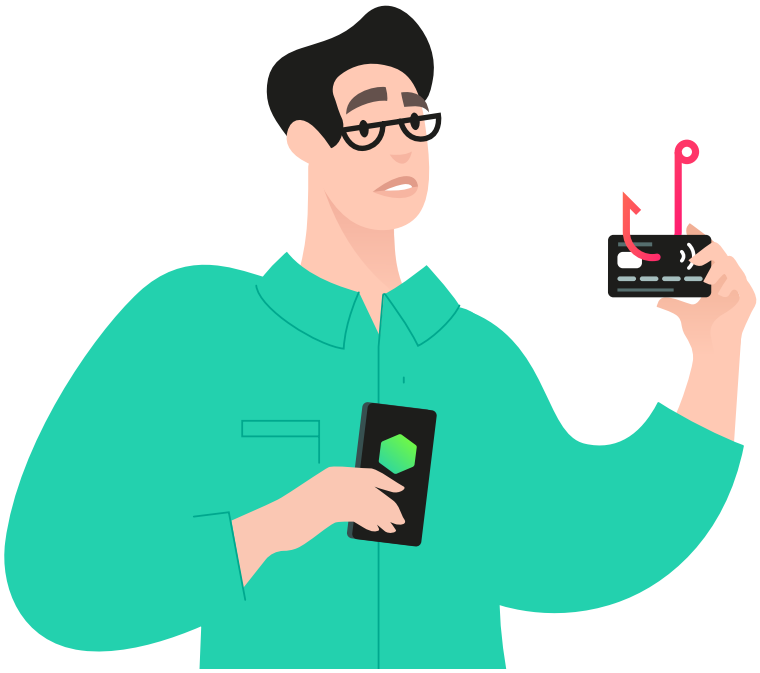
[6] You can find more information at https://securelist.com/spam-and-phishing-in-q2-2020/97987/

Nigerian scams
Of course, scammers simply couldn't ignore the lucrative subject of COVID-19: philanthropists and dying millionaires offered rewards for facilitating the withdrawal of funds that would go to humanitarian aid. In addition, recipients were invited to help with the production of a miracle vaccine that had already been developed or to participate in a charity raffle, the proceeds of which would go to help poor people affected by the pandemic.

You can find more information at https://securelist.com/spam-and-phishing-in-q1-2020/97091/

To avoid revealing their cards right away, the scammers used services to shorten links and spread messages on social networks and messengers where shortened links look more natural.

In their messages the scammers offered cheap trips or hotel stays at bargain prices. And it's impossible to know where the link in such a message leads to without clicking it, which is exactly what the attackers were counting on.



The pandemic theme, which started in phishing and spam in the first quarter of the year, is still a major topic. We believe the second wave of COVID-19 may cause a flurry of mailings offering products to prevent and treat the coronavirus. Meanwhile, as the economic situation worsens, there may be an increase in the number of fraudulent mailings with requests for small payments that will quickly add up to a considerable profit.

Money laundering

An attack on banks can take two forms: directly against the bank infrastructure and accounts, or against ATMs and related systems. Of course, the withdrawal and subsequent money laundering schemes differ slightly. But the result is the same — the attackers will try to integrate the stolen funds back into legitimate circulation.

The last stage, the integration of already laundered funds back into the economy, is a separate topic that deserves its own separate study. Therefore, we won't discuss it in detail here. But there is another stage, the zero stage: long before the money is stolen and the mechanisms for legalizing it come into play, the process of preparation begins.

In forensics, the direct process of money laundering is traditionally divided into three stages: placement, layering and integration.

Preparation

In order to quickly transfer the stolen funds, criminals usually prepare multiple accounts belonging to individuals or legal entities. These may be the accounts of unsuspecting individuals that cybercriminals have gained access to, or of people tricked into participating in fraudulent activity, or willing accomplices of the cybercriminals.

People who assist the perpetrators are commonly referred to as mules. Sometimes they are used to open accounts with forged or stolen documents (of course, the criminals must have an insider to prevent the bank from recognizing the forgery). Mules are often recruited through recruitment agencies that mask the blatant illegality of the offer with vague expressions like "organizing convenient methods of investment". In reality, these people, usually know perfectly well that they are participating in something illegal, but prefer to turn a blind eye — the offer is just too good to refuse.

Placement

Once the cybercriminals have transferred the stolen money to an account the mules come into play. They act in the following way:

- move funds to other accounts to throw potential trackers off the scent;
- order goods to their own address (or to an address that they have access to in some way);
- withdraw money from ATMs.

Layering

When accomplices who are in the loop receive the goods or money, they use long-established criminal practices to legalize the booty. Money may be exchanged for freely convertible currency (typically dollars); goods (typically electronics) are sold directly to buyers or second-hand stores. Of course, currency exchange offices and stores that buy items are supposed to have mechanisms in place to detect illegal transactions, but either negligence or insiders can bypass them. A third party then transfers the money to the organizers of the scheme. Of course, mules can be caught. But the most that the authorities can seize are the mules themselves and their percentage. Meanwhile, the bulk of the proceeds — and the masterminds — remain elusive.

Next, the money is laundered using classic criminal methods such as buying jewelry or metals (those businesses still often prefer dealing in cash), or buying and selling chips in a casino.

If the money remains in non-cash form through further transfers, then the process involves shell companies operating globally. Such businesses are usually located in countries that lack tight control over financial transactions, or where strict laws protect the secrecy of commercial dealings. A few more transfers, involving splitting and converting into different currencies, obscure the origin of the money. The firms are not necessarily fly-by-night operations — they may have a partially legitimate business into which the stolen money flows under the radar.

Cryptocurrencies joined the list of money-laundering tools fairly recently. Cybercriminals are drawn to them because users need not provide personal data to complete transactions. However, using cryptocurrencies for laundering money isn't as easy as it seems. After all, along with anonymity, blockchain-based currency also comes with complete transparency. That means withdrawing funds requires a lot of transactions. In 2018, for example, the Lazarus group withdrew $30 million after hacking a cryptocurrency exchange, then made 68 transfers in four days between different wallets.

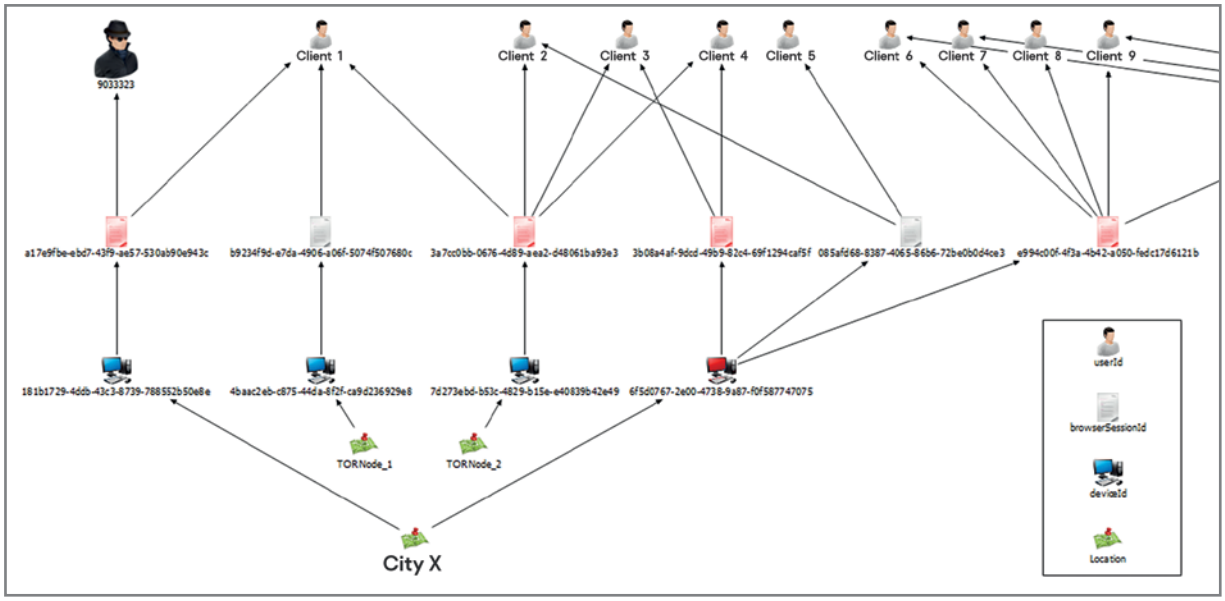
For sophisticated money laundering schemes, scammers use automation tools, proxy servers, remote administration tools and TOR browsers to cover their tracks and remain anonymous or to avoid being caught in a previously detected drop network. Our team of analysts concluded that the growth in attempts to launder money is related to the ongoing reduction in the number of banks in Russia, the availability of fraud tools on the internet (laundering and fraud as a service), as well as the number of leaks of personal data belonging to bank customers and their subsequent circulation on the internet.

The following is part of a scheme that illustrates the core algorithm for 'promoting' fraud:

- Detected drop accounts are colored black. What is important here is separating the attacker's account from the victim's. The drop account or presumed attacker can be identified by using session antifraud solutions or by analyzing transactions initiated by the account.
- Once one drop account has been identified, the capabilities and technology offered by the session antifraud solution must be put to use.

The key elements that helped to identify interlinked drop net users by using session antifraud data are marked red in the chart.

12



Practical takeaways

As we can see, cybercriminals have built complex, multistage money laundering schemes in which they juggle accounts, companies, legal form, currency, and jurisdiction — all within a matter of days, during which some companies don't even know they have been attacked.

Therefore, it makes sense for banks to take matters into their own hands and create cybersecurity infrastructures that minimize the chances of financial systems being hacked and hijacked.[7]

[7] You can find out more at https://www.kaspersky.com/blog/money-laundering-schemes/37175/

E-commerce fraud

13

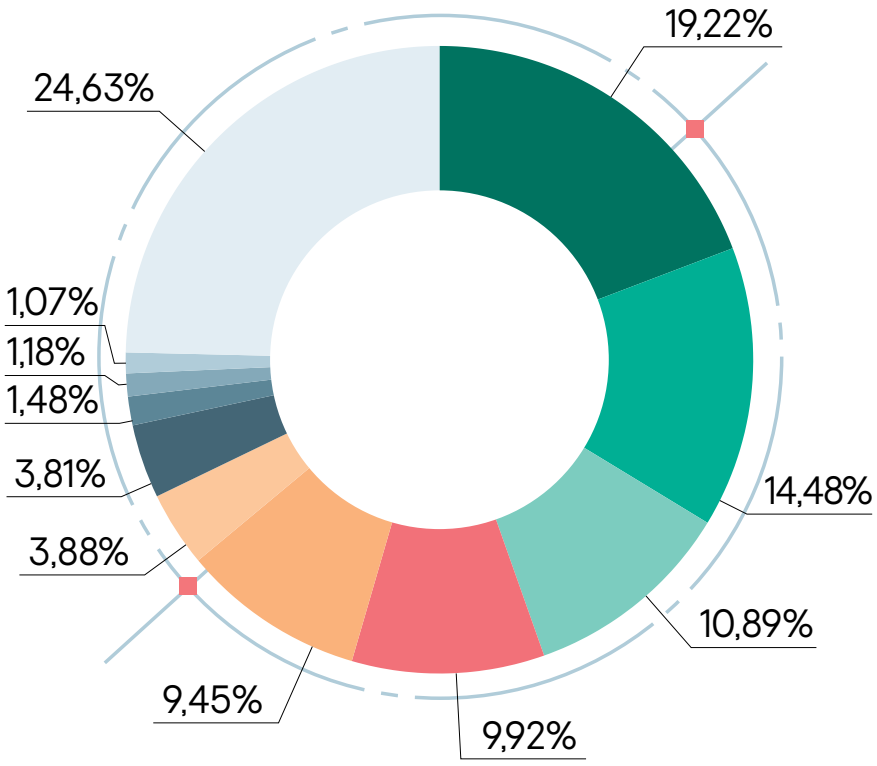
The country with the highest percentage of users attacked by phishers was Mongolia (15.54%).

In second place, by a small margin, was Israel (15.24%), followed by France (12.57%) in third.

- Online stores
- Global internet portals
- Banks
- Social networks
- E-payment systems
- Telecommunication companies
- IMS
- Financial services
- Online games
- Logistics companies
- Other

Organizations targeted by phishing attacks

The largest number of phishing attacks were on organizations in the 'Online stores' category. Compared to the second quarter of 2020, its share decreased slightly (by 0.2 p.p.) to 19.22%.[8]



Distribution of organizations affected by phishing attacks by category, Q3 2020

Welcome fraud

One of the most striking cases of cross-organizational cyberfraud exposed recently was the discovery of a network of 3,029 fraudulent accounts. The main goal of the criminals was to receive bonus points by creating a large number of accounts on an online portal. The criminals bought codes for replenishing their accounts in a gaming store and then sold them online on social networks and marketplaces. We noticed that all of the criminals performed their operations manually, and our research detected 14 devices showing mass login attempts (10 to 65 unique users).

During our research, user accounts and devices were combined for the purpose of analyzing user activity, and we detected an enormous cluster of 11,256 unique users.

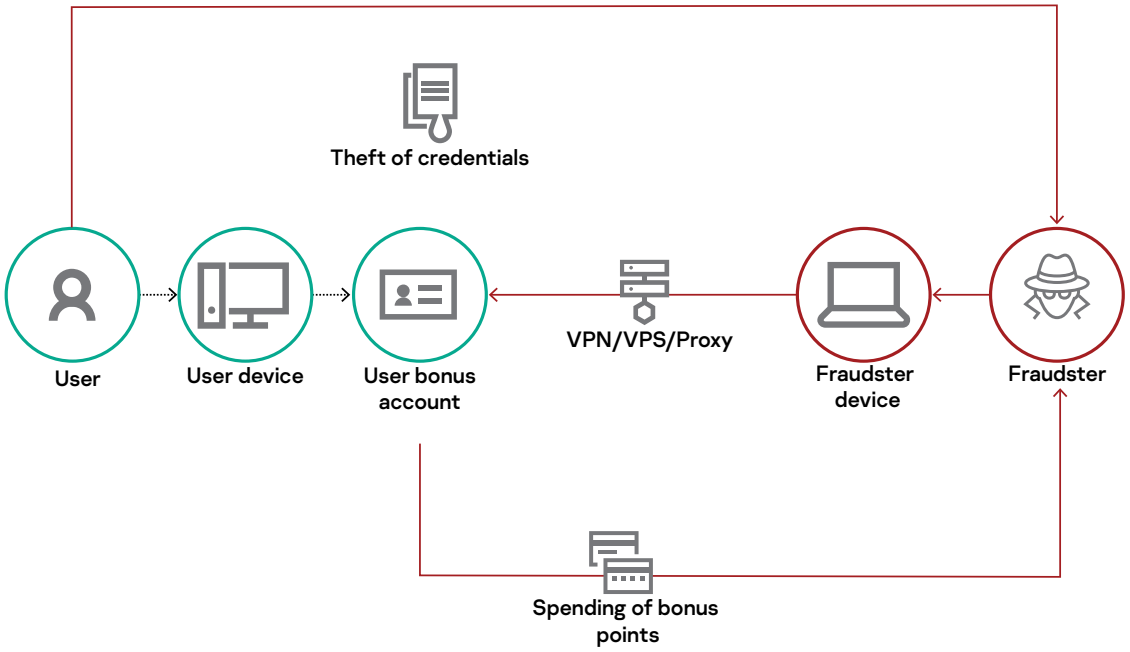
Another fraud technique is related to the abuse of welcome bonuses in loyalty programs. The scheme is fairly simple: scammers register accounts on the marketplace en masse, receive their welcome bonus points and get goods at a reduced price. One such abuser bought up nappies and candy, subsequently selling these on classified advertisements websites at a profit. The accounts were later abandoned, their average lifetime being one or two days.

[8] You can find out more at https://securelist.com/spam-and-phishing-in-q3-2020/99325/

Compromise of a loyalty program account

The compromise of a bonus system account usually occurs in three ways: a targeted attack on a personal account (brute force), collateral compromise via other services (email account), or with the help of Trojan stealers. The attacker then enters the personal account, preventing the owner from restoring access by changing the contact information, and subsequently manages the bonus account, performing the following types of transactions:

14

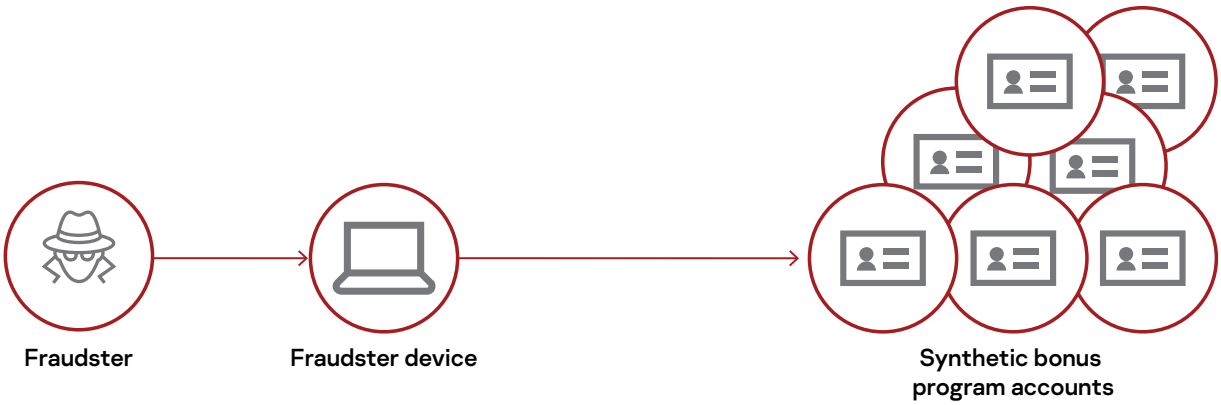


- Bonus points stolen by transferring them to other accounts (if the bonus program allows transfers).
- Bonus points spent on purchases/orders issued to other accounts, addresses, etc.
- Use of various privileges available to the compromised account (discounts, gifts, etc.).
- Sale of a compromised account to other interested parties on sites with a related theme.

Synthetic loyalty program accounts

The creation of synthetic (fake) accounts is relatively easy for scammers and at the same time provides lots of opportunities to commit fraud. Fraudsters can use or resell welcome bonuses, promo codes or other gifts received upon registration or they can boost their chances of winning a prize in promos by participating from multiple accounts.

15



If a bonus program participant only uses a physical bonus card, the fraudster (armed with the bonus card data) can create a new, fake account, attach it to the card and steal the user's accumulated bonus points.

Sometimes synthetic accounts can be used with various partner programs for fraudulent schemes involving advertising traffic.

Then there is the creation of synthetic accounts by "resellers" of goods that are bought using a welcome bonus and then resold on other sites; this also comes with the added benefit of more loyalty program bonus points and, for example, cashback to the bank card used to make the purchase.

The economic aspect of cybersecurity

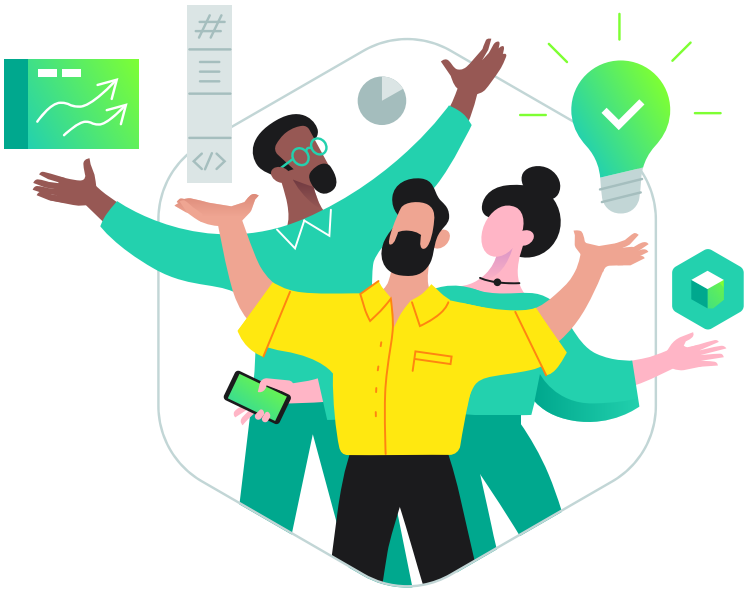
Results of the annual Kaspersky Global Corporate IT Security Risks Survey

Large enterprise-level companies cut cybersecurity spending from an average of $18.9 million last year to $14 million in 2020. And this is despite the fact that the proportion of IT budget spending allocated to security has increased in percentage terms. Of course, this was expected because almost all companies faced unexpected costs and losses due to quarantine. The SMB picture is different: security budgets there increased slightly (from $267,000 in 2019 to $275,000 in 2020).

A total of 71% of companies plan to increase their investments in security over the next three years. What's more, regardless of company size, respondents cited the increased complexity of IT infrastructure and the need to increase employee expertise as the main reasons for the increase. 17% hope to keep cybersecurity outlays at the same level, and only the remaining 12% are considering further budget cuts as part of an overall optimization or in the belief that past investments have already helped solve the key issues.[9]

The Total Economic Impact™ Of Kaspersky Fraud Prevention

To better understand the benefits, costs and risks associated with this investment, Forrester interviewed one customer with more than two years of experience using Kaspersky Fraud Prevention.



Prior to using the solution, the interviewed customer did not have a fraud prevention solution in the digital channel. Due to a spike in fraudulent activities seen at financial services companies, the interviewed organization was concerned about the possibility of fraud and its effect on customers, the organization's reputation, potential customer churn, and investigation and recovery expenses.

As a result of implementing and actively using the Advanced Authentication and Automated Fraud Analytics components, the organization reduced fraud and achieved a more frictionless CX.

[9] You can find out more at https://www.kaspersky.com/blog/it-security-economics-2020-main/37205/

Key Findings

- **Reduced fraud losses, totaling $3.4 million over three years.** Kaspersky Fraud Prevention allowed the interviewed organization to identify and prevent fraudulent activity in the online channel.
- **Savings in customer service interactions, totaling $121K over three years.** Using the Advanced Authentication component of the Kaspersky Fraud Prevention allowed the organization to build an "easy entrance" mechanism where customers could authenticate directly from their desktops with the same level of security as could be achieved from a call to the call center, foregoing the additional calls.
- **Savings from eliminating second-tier authentication for verified customers, totaling $17.6K over three years.** Kaspersky Fraud Prevention eliminated the need for extra verification steps for most legitimate users, allowing the organization to make CX more seamless and minimize hurdles for customers to access their online accounts, while keeping fraud risks low.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $3.6 million over three years versus costs of $1.3 million, adding up to a net present value (NPV) of $2.2 million and an ROI of 168%.

For more information about this research, as well as about Kaspersky Fraud Prevention, visit our website at kfp.kaspersky.com

IT Security News:
www.kaspersky.com/blog
Cyber Threats News:
www.securelist.com

@KasperskyFP

www.kaspersky.com

TOP 100

Kaspersky Fraud Prevention is among top 100 best inventions of 2017 according to Rospatent: https://kas.pr/100best

Kaspersky Fraud Prevention Automated Fraud Analytics [156555] included in the Register by Order of the Ministry of Communications of the Russian Federation dated November 19, 2019 No. 742, Appendix 1, No. 72, registry number 5954
Kaspersky Fraud Prevention Advanced Authentication [156556] included in the Register by Order of the Ministry of Communications of the Russian Federation dated November 19, 2019 No. 742, Appendix 1, No. 73, registry number 5955

WORLD BRANDING AWARDS
BRAND OF THE YEAR

GBD-416.Q120.V1_RU