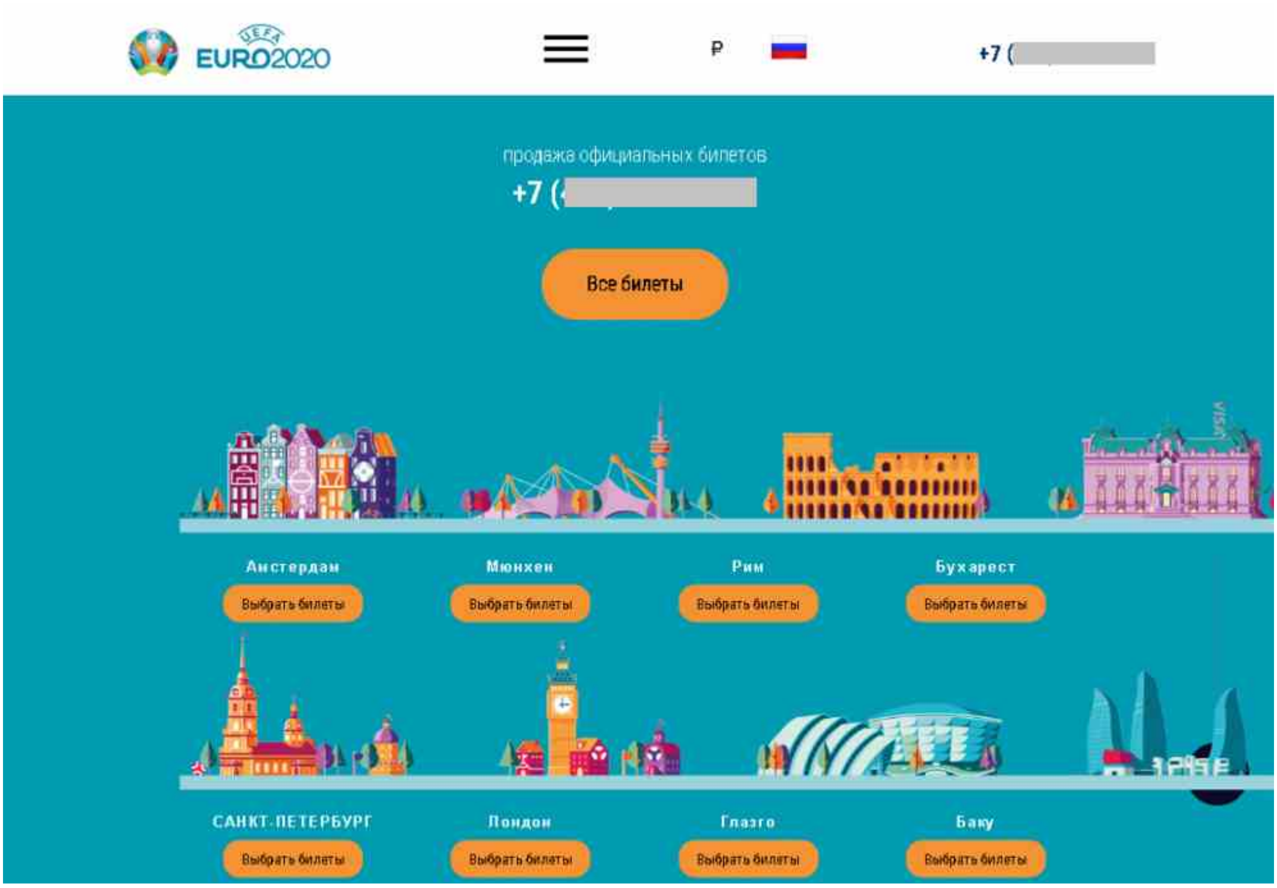
Spam and phishing in Q3 2021

securelist.com/spam-and-phishing-in-q3-2021/104741

Quarterly highlights

Scamming championship: sports-related fraud

This summer and early fall saw some major international sporting events. The delayed Euro 2020 soccer tournament was held in June and July, followed by the equally delayed Tokyo Olympics in August. Q3 2021 also featured several F1 Grand Prix races. There was no way that cybercriminals and profiteers could pass up such a golden opportunity. Fans wanting to attend events live encountered fake ticket-selling websites. Some sites made a point of stressing the tickets were "official", despite charging potential victims several times the real price of a ticket, and some just took the money and disappeared.



UEFA EURO2020

₽

+7 ([redacted]

продажа официальных билетов

+7 ([redacted]

Все билеты

Амстердам

Выбрать билеты

Мюнхен

Выбрать билеты

Рим

Выбрать билеты

Бухарест

Выбрать билеты

САНКТ-ПЕТЕРБУРГ

Выбрать билеты

Лондон

Выбрать билеты

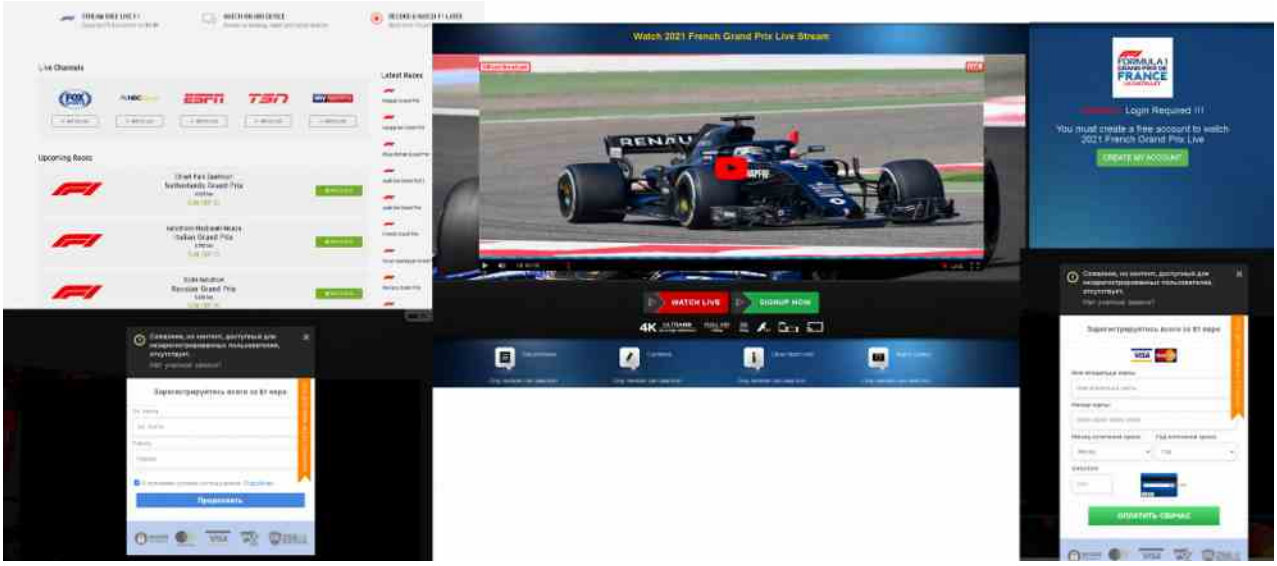
Глазго

Выбрать билеты

Баку

Выбрать билеты

Scammers also laid traps for those preferring to watch the action online from the comfort of home. Fraudulent websites popped up offering free live broadcasts. On clicking the link, however, the user was asked to pay for a subscription. If that did not deter them, their money and bank card details went straight to the scammers, with no live or any other kind of broadcast in return. This scheme has been used many times before, only instead of sporting events, victims were offered the hottest movie and TV releases.



Live Channels

Upcoming Races

Latest Races

Netherlands Grand Prix

Italian Grand Prix

Russian Grand Prix

Watch 2021 French Grand Prix Live Stream

Login Required !!!

You must create a free account to watch 2021 French Grand Prix Live

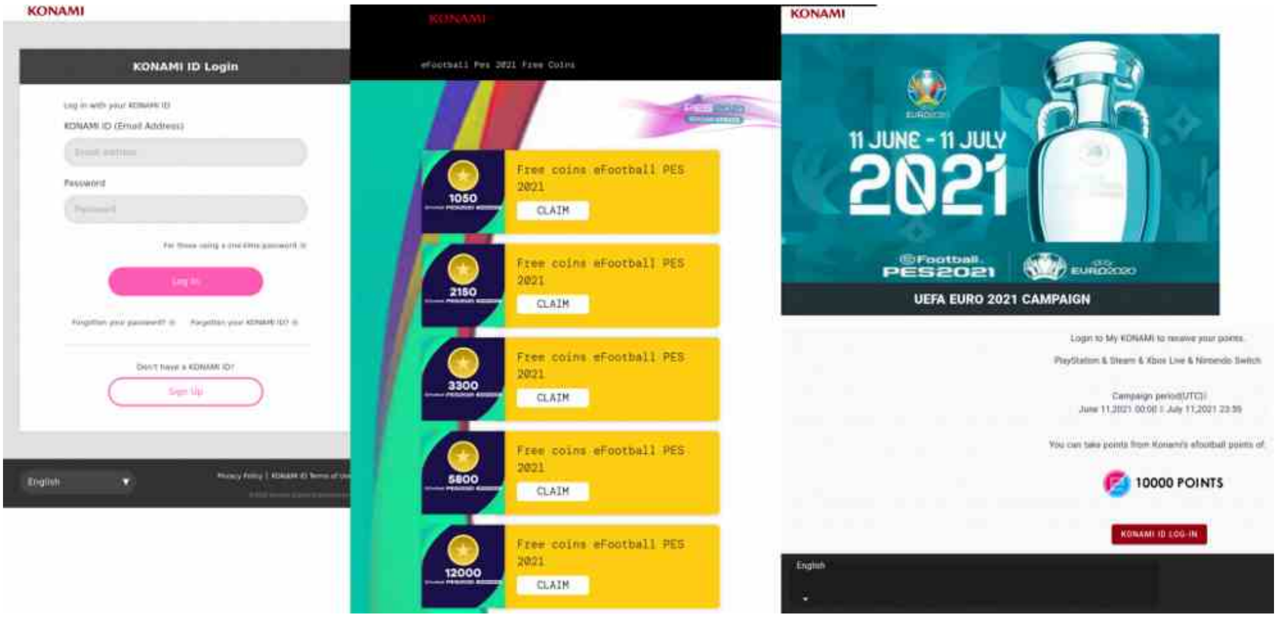
CREATE MY ACCOUNT

WATCH LIVE

SIGNUP NOW

Продолжить

Soccer video games always attract a large following. This success has a downside: gaming platforms get attacked by hackers, especially during major soccer events. Accordingly, the Euro 2020 championship was used by scammers as bait to hijack accounts on the major gaming portal belonging to Japanese gaming giant Konami. The cybercriminals offered users big bonuses in connection with the tournament. However, when attempting to claim the bonus, the victim would land on a fake Konami login page. If they entered their credentials, the attackers took over their account and the “bonus” evaporated into thin air.


KONAMI
KONAMI ID Login
Log in with your KONAMI ID
KONAMI ID (Email Address)
Password
Log in
Don't have a KONAMI ID?
Sign Up
English
KONAMI
eFootball Pes 2021 Free Coins
1050
Free coins eFootball PES 2021
CLAIM
2150
Free coins eFootball PES 2021
CLAIM
3300
Free coins eFootball PES 2021
CLAIM
5800
Free coins eFootball PES 2021
CLAIM
12000
Free coins eFootball PES 2021
CLAIM
KONAMI
11 JUNE - 11 JULY
2021
eFootball PES2021
EURO2020
UEFA EURO 2021 CAMPAIGN

Login to My KONAMI to receive your points.

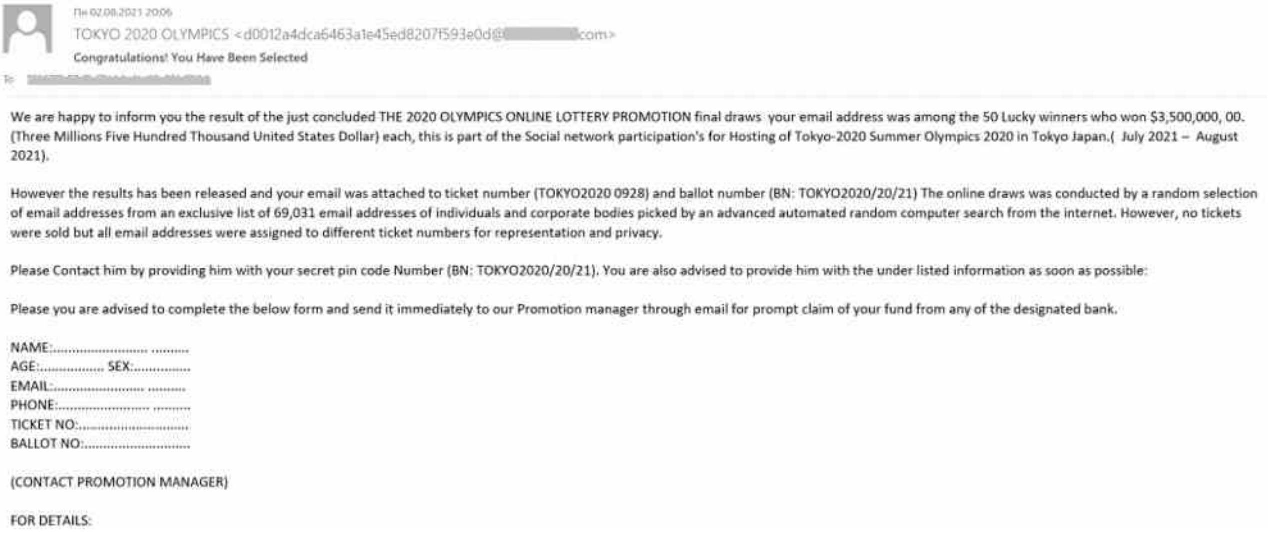
PlayStation & Steam & Xbox Live & Nintendo Switch

Campaign period(UTC):
June 11,2021 00:00 ~ July 11,2021 23:59

You can take points from Konami's efootball points of.

10000 POINTS

“Nigerian prince” scammers also had a close eye on Q3’s sporting fixture. The e-mails that came to our attention talked about multi-million-dollar winnings in Olympics-related giveaways. To receive the prize, victims were asked to fill out a form and e-mail it to the cybercriminals.



Пн 02.08.2021 20:06
TOKYO 2020 OLYMPICS <d0012a4dca6463a1e45ed8207f593e0d@[redacted]com>
Congratulations! You Have Been Selected
To [redacted]

We are happy to inform you the result of the just concluded THE 2020 OLYMPICS ONLINE LOTTERY PROMOTION final draws your email address was among the 50 Lucky winners who won $3,500,000, 00. (Three Millions Five Hundred Thousand United States Dollar) each, this is part of the Social network participation's for Hosting of Tokyo-2020 Summer Olympics 2020 in Tokyo Japan.(July 2021 – August 2021).

However the results has been released and your email was attached to ticket number (TOKYO2020 0928) and ballot number (BN: TOKYO2020/20/21) The online draws was conducted by a random selection of email addresses from an exclusive list of 69,031 email addresses of individuals and corporate bodies picked by an advanced automated random computer search from the internet. However, no tickets were sold but all email addresses were assigned to different ticket numbers for representation and privacy.

Please Contact him by providing him with your secret pin code Number (BN: TOKYO2020/20/21). You are also advised to provide him with the under listed information as soon as possible:

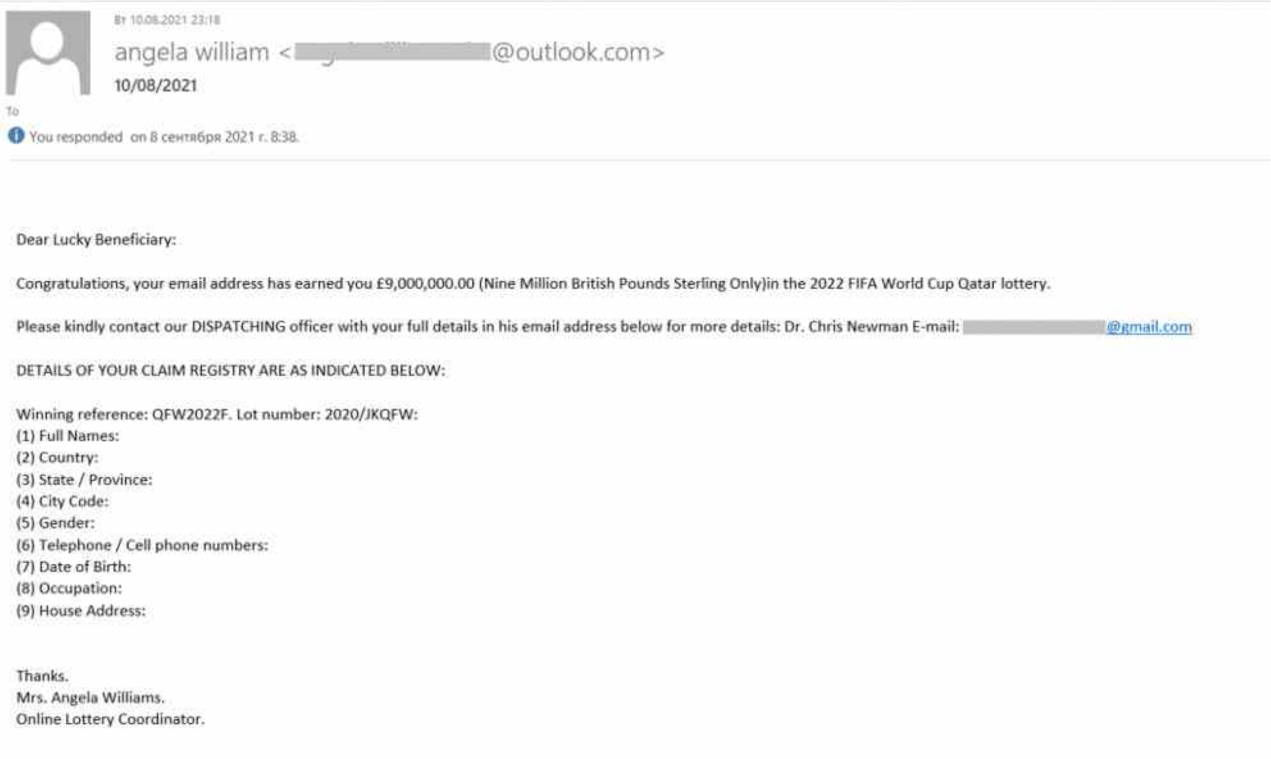
Please you are advised to complete the below form and send it immediately to our Promotion manager through email for prompt claim of your fund from any of the designated bank.

NAME:............................ ....
AGE:................. SEX:...............
EMAIL:........................... ....
PHONE:.......................... ....
TICKET NO:..............................
BALLOT NO:.............................

(CONTACT PROMOTION MANAGER)

FOR DETAILS:

Some messages anticipated upcoming events in the world of sport. The FIFA World Cup is slated for far-off November — December 2022, yet scammers are already inventing giveaways related to it.



Вт 10.08.2021 23:18

angela william <[redacted]@outlook.com>

10/08/2021

To

You responded on 8 сентября 2021 г. 8:38.

Dear Lucky Beneficiary:

Congratulations, your email address has earned you £9,000,000.00 (Nine Million British Pounds Sterling Only)in the 2022 FIFA World Cup Qatar lottery.

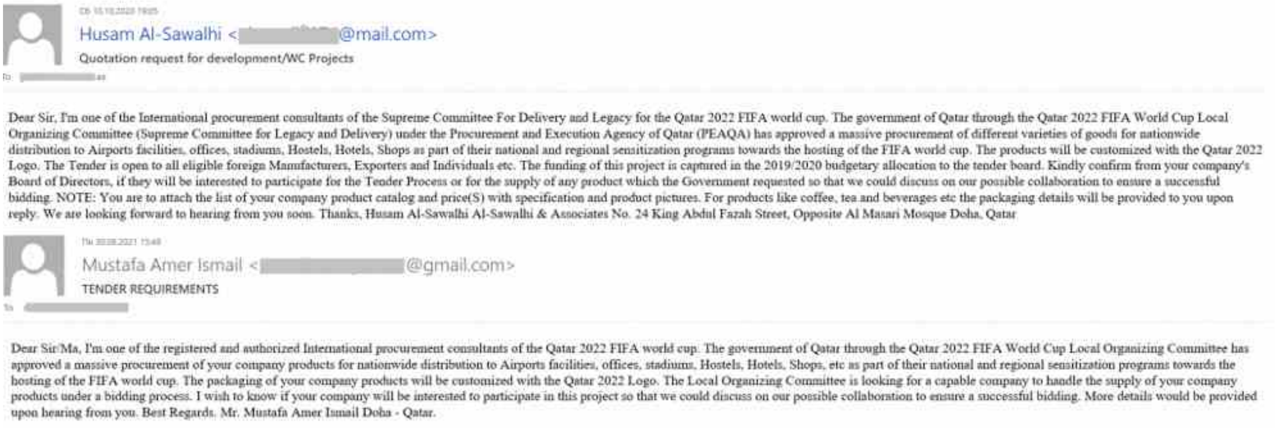
Please kindly contact our DISPATCHING officer with your full details in his email address below for more details: Dr. Chris Newman E-mail: [redacted]@gmail.com

DETAILS OF YOUR CLAIM REGISTRY ARE AS INDICATED BELOW:

Winning reference: QFW2022F. Lot number: 2020/JKQFW:
(1) Full Names:
(2) Country:
(3) State / Province:
(4) City Code:
(5) Gender:
(6) Telephone / Cell phone numbers:
(7) Date of Birth:
(8) Occupation:
(9) House Address:

Thanks.
Mrs. Angela Williams.
Online Lottery Coordinator.

Among other things, we found some rather unusual spam e-mails with an invitation to bid for the supply of products to be sold at airports and hotels during the World Cup. Most likely, the recipients would have been asked to pay a small commission to take part in the bidding or giveaway, with no results ever coming forth.



[illegible]

Husam Al-Sawalhi <[redacted]@mail.com>

Quotation request for development/WC Projects

To [redacted]

Dear Sir, I'm one of the International procurement consultants of the Supreme Committee For Delivery and Legacy for the Qatar 2022 FIFA world cup. The government of Qatar through the Qatar 2022 FIFA World Cup Local Organizing Committee (Supreme Commitee for Legacy and Delivery) under the Procurement and Execution Agency of Qatar (PEAQA) has approved a massive procurement of different varieties of goods for nationwide distribution to Airports facilities, offices, stadiums, Hostels, Hotels, Shops as part of their national and regional sensitization programs towards the hosting of the FIFA world cup. The products will be customized with the Qatar 2022 Logo. The Tender is open to all eligible foreign Manufacturers, Exporters and Individuals etc. The funding of this project is captured in the 2019/2020 budgetary allocation to the tender board. Kindly confirm from your company's Board of Directors, if they will be interested to participate for the Tender Process or for the supply of any product which the Government requested so that we could discuss on our possible collaboration to ensure a successful bidding. NOTE: You are to attach the list of your company product catalog and price(S) with specification and product pictures. For products like coffee, tea and beverages etc the packaging details will be provided to you upon reply. We are looking forward to hearing from you soon. Thanks, Husam Al-Sawalhi Al-Sawalhi & Associates No. 24 King Abdul Fazah Street, Opposite Al Masari Mosque Doha, Qatar

[illegible]

Mustafa Amer Ismail <[redacted]@gmail.com>

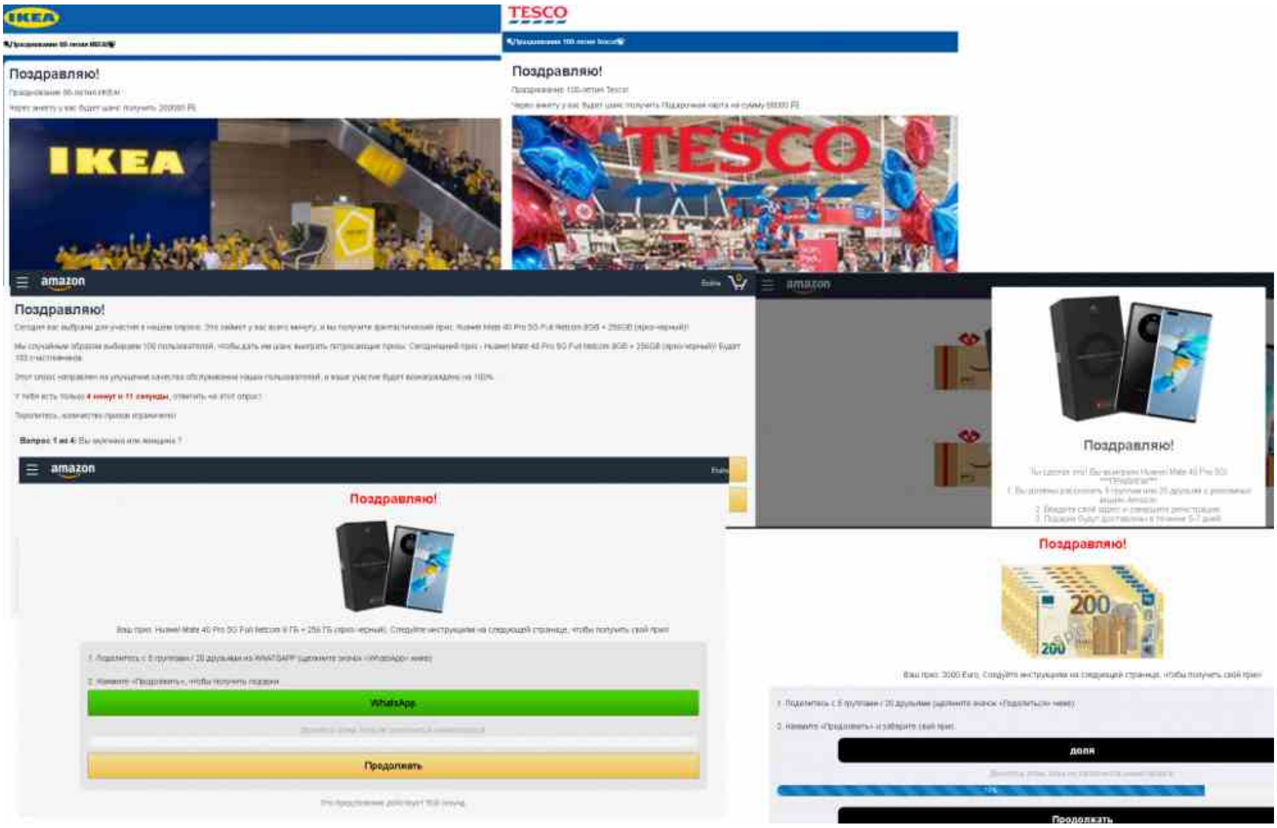
TENDER REQUIREMENTS

To [redacted]

Dear Sir/Ma, I'm one of the registered and authorized International procurement consultants of the Qatar 2022 FIFA world cup. The government of Qatar through the Qatar 2022 FIFA World Cup Local Organizing Committee has approved a massive procurement of your company products for nationwide distribution to Airports facilities, offices, stadiums, Hostels, Hotels, Shops, etc as part of their national and regional sensitization programs towards the hosting of the FIFA world cup. The packaging of your company products will be customized with the Qatar 2022 Logo. The Local Organizing Committee is looking for a capable company to handle the supply of your company products under a bidding process. I wish to know if your company will be interested to participate in this project so that we could discuss on our possible collaboration to ensure a successful bidding. More details would be provided upon hearing from you. Best Regards. Mr. Mustafa Amer Ismail Doha - Qatar.

Scam: get it yourself, share with friends

In Q3 2021, our solutions blocked more than 5.6 million redirects to phishing pages. Anniversaries of well-known brands have become a favorite topic for attackers. According to announcements on fake sites, IKEA, Amazon, Tesco and other companies all held prize draws to celebrate a milestone date. Wannabe participants had to perform a few simple actions, such as taking a survey or a spot-the-hidden-prize contest, or messaging their social network contacts about the promotion, and then were asked to provide card details, including the CVV code, to receive the promised payout. That done, the attackers not only got access to the card, but also requested payment of a small commission to transfer the (non-existent) winnings. Curiously, the scammers came up with fake round dates, for example, the 80th anniversary of IKEA, which in reality will come two years later. It is always advisable to check promotions on official websites, rather than trusting e-mails, which are easy to spoof.



Поздравляю!

Поздравляю!

Поздравляю!

Вопрос 1 из 4:

Поздравляю!

WhatsApp

Продолжать

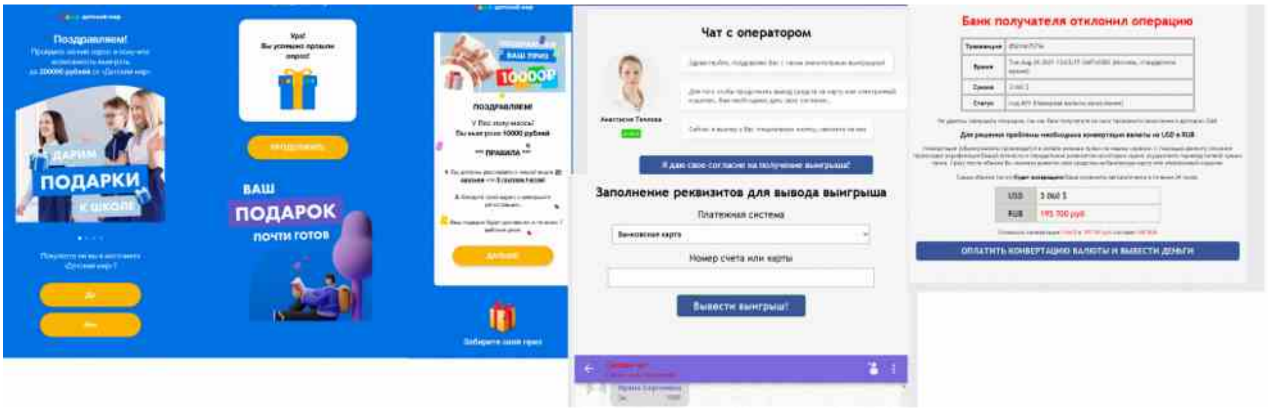
Поздравляю!

Поздравляю!

доля

Продолжать

There were also plenty of “holiday deals” supposedly from major Russian brands, with some, it seemed, showing particular generosity in honor of September 1, or Knowledge Day, when all Russian schools and universities go back after the summer break. Those companies allegedly giving away large sums were all related to education in one way or another. At the same time, the fraudulent scheme remained largely the same, with just some minor tinkering round the edges. For example, fake Detsky Mir (Children’s World, a major chain of kids’ stores) websites promised a fairly large sum of money, but on condition that the applicant sends a message about the “promotion” to 20 contacts or 5 groups. And the payment was then delayed, allegedly due to the need to convert dollars into rubles: for this operation, the “lucky ones” had to pay a small fee.



Поздравляем!

Ура!

*** ПРАВИЛА ***

Чат с оператором

Я даю свое согласие на получение выигрыша!

Заполнение реквизитов для вывода выигрыша

Платежная система

Банковская карта

Номер счета или карты

Вывести выигрыш!

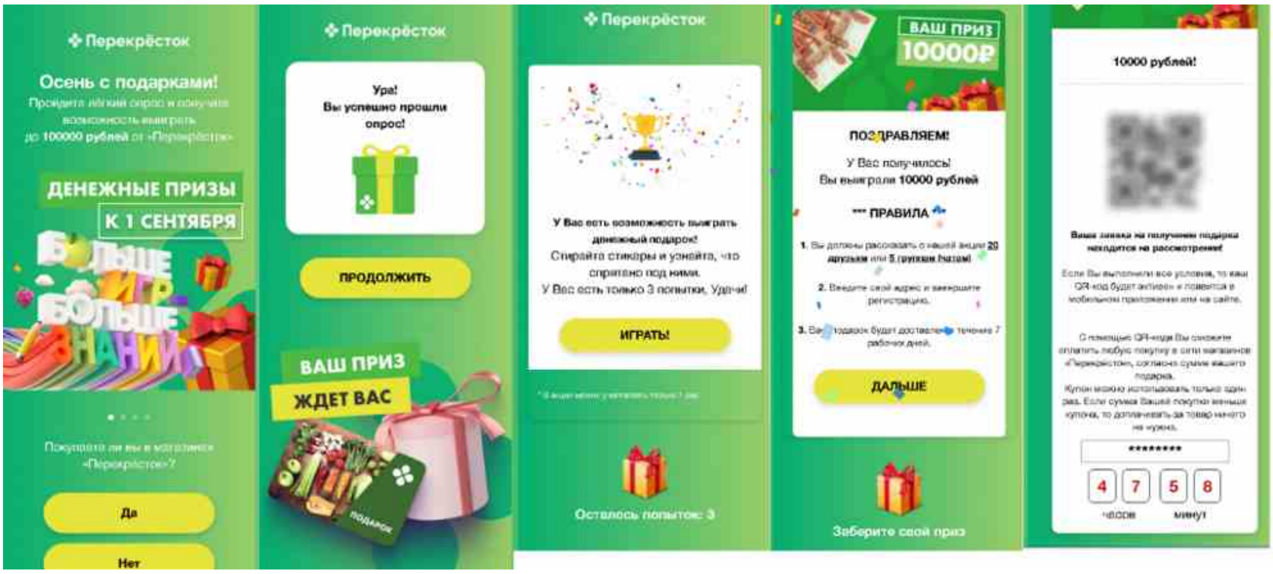
Банк получателя отклонил операцию

Для решения проблемы необходима конвертация валюты из USD в RUB

USD	3 060 $
RUB	195 700 руб

ОПЛАТИТЬ КОНВЕРТАЦИЮ ВАЛЮТЫ И ВЫВЕСТИ ДЕНЬГИ

On a fake website holding a giveaway under the Perekrestok brand, after completing the tasks the “winner” was promised as a prize a QR code that could supposedly be used to make purchases in the company’s stores. Note that Perekrestok does indeed issue coupons with QR codes to customers; that is, the cybercriminals tried to make the e-mail look plausible. When trying to retrieve this code, the potential victim would most likely be asked to pay a “commission” before being able to spend the prize money. Note too that QR codes from questionable sources can carry other threats, for example, spreading malware or debiting money in favor of the scammers.


Перекрёсток

Осень с подарками!

Пройдите лёгкий опрос и получите возможность выиграть до 100000 рублей от «Перекрёстка»

Покупаете ли вы в магазинах «Перекрёсток»?

Ура!
Вы успешно прошли опрос!

У Вас есть возможность выиграть денежный подарок!
Стирайте стикеры и узнайте, что спрятано под ними.
У Вас есть только 3 попытки, Удачи!

* В акции можно участвовать только 1 раз

Осталось попыток: 3

ПОЗДРАВЛЯЕМ!

У Вас получилось!
Вы выиграли 10000 рублей

*** ПРАВИЛА

1. Вы должны рассказать о нашей акции 20 друзьям или 5 группам (чатам)
2. Введите свой адрес и завершите регистрацию.
3. Ваш подарок будет доставлен в течение 7 рабочих дней.

Заберите свой приз

10000 рублей!

Ваша заявка на получение подарка находится на рассмотрении!

Если Вы выполнили все условия, то ваш QR-код будет активен и появится в мобильном приложении или на сайте.

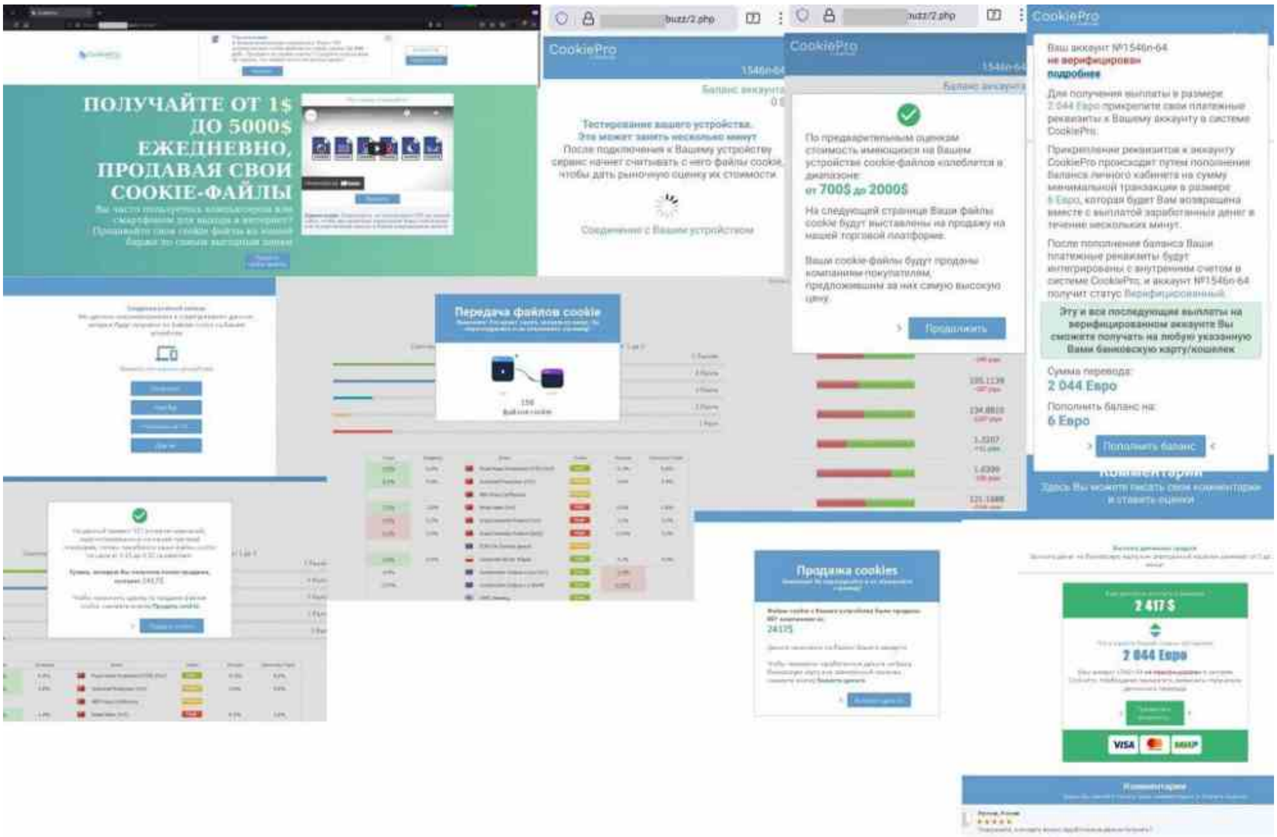
С помощью QR-кода Вы сможете оплатить любую покупку в сети магазинов «Перекрёсток», согласно сумме вашего подарка.
Купон можно использовать только один раз. Если сумма Вашей покупки меньше купона, то доплачивать за товар ничего не нужно.

****

In 2021, there was an increase in the number of fake resources posing as cookie-selling platforms. Users were promised a generous monetary reward (up to $5,000 a day) for selling such data. Those who fell for the tempting offer and followed the link were redirected to a fake page that allegedly “reads cookies from the victim’s device to estimate their market value.” The “valuation” most often landed in the US$700–2,000 range. To receive this money, the user was asked to put the cookies up at a kind of auction, in which different companies were allegedly taking part. The scammers assured that the data would go to the one offering the highest price.

If the victim agreed, they were asked to link their payment details to the account in the system and to top it up by €6, which the scammers promised to return, together with the auction earnings, within a few minutes. To top up the balance, the victim was required to enter their bank card details into an online form. Naturally, they received no payment, and the €6 and payment details remained in the attackers’ possession.

Note that the very idea of selling cookies from your device is risky: these files can store confidential information about your online activity — in particular, login details that let you avoid having to re-enter your credentials on frequently used sites.



ПОЛУЧАЙТЕ ОТ 1$ ДО 5000$ ЕЖЕДНЕВНО, ПРОДАВАЯ СВОИ COOKIE-ФАЙЛЫ

[redacted]buzz/2.php

CookiePro

Баланс аккаунта

Тестирование вашего устройства.
Это может занять несколько минут
После подключения к Вашему устройству сервис начнет считывать с него файлы cookie, чтобы дать рыночную оценку их стоимости.

Соединение с Вашим устройством

[redacted]buzz/2.php

CookiePro

1546n-64

Баланс аккаунта

По предварительным оценкам стоимость имеющихся на Вашем устройстве cookie-файлов колеблется в диапазоне:
от 700$ до 2000$

На следующей странице Ваши файлы cookie будут выставлены на продажу на нашей торговой платформе.

Ваши cookie-файлы будут проданы компаниям-покупателям, предложившим за них самую высокую цену.

Продолжить

CookiePro

Ваш аккаунт №1546n-64
не верифицирован
подробнее

Для получения выплаты в размере 2 044 Евро прикрепите свои платежные реквизиты к Вашему аккаунту в системе CookiePro.

Прикрепление реквизитов к аккаунту CookiePro происходит путем пополнения баланса личного кабинета на сумму минимальной транзакции в размере 6 Евро, которая будет Вам возвращена вместе с выплатой заработанных денег в течение нескольких минут.

После пополнения баланса Ваши платежные реквизиты будут интегрированы с внутренним счетом в системе CookiePro, и аккаунт №1546n-64 получит статус Верифицированный.

Эту и все последующие выплаты на верифицированном аккаунте Вы сможете получать на любую указанную Вами банковскую карту/кошелек

Сумма перевода:
2 044 Евро

Пополнить баланс на:
6 Евро

Пополнить баланс

Комментарии
Здесь Вы можете писать свои комментарии и ставить оценки

Передача файлов cookie

Продажа cookies

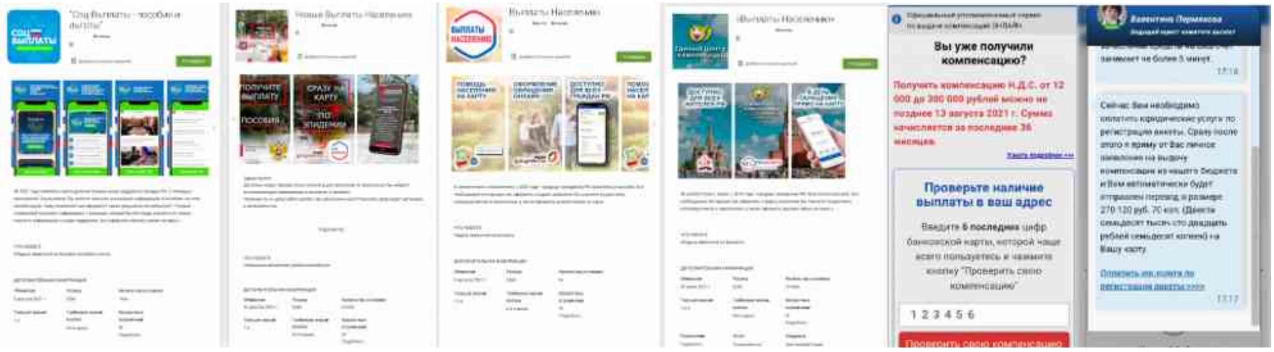
24175

2 417 $

2 044 Евро

Комментарии

Even in official mobile app stores, malware can sometimes sneak in. As such, this quarter saw a new threat in the shape of fraudulent welfare payment apps that could be downloaded on such platform. The blurb described them as software that helps find and process payments from the government that the user is entitled to. Due payments (fake, of course) were indeed found, but to receive the money, the user was requested to "pay for legal services relating to form registration". The numerous positive reviews under the application form, as well as the design mimicking real government sites, added credibility. We informed the store in question, which they removed the fraudulent apps.



Вы уже получили компенсацию?

Получить компенсацию Н.Д.С. от 12 000 до 300 000 рублей можно не позднее 13 августа 2021 г. Сумма начисляется за последние 36 месяцев.

Проверьте наличие выплаты в ваш адрес

Введите 6 последних цифр банковской карты, которой чаще всего пользуетесь и нажмите кнопку "Проверить свою компенсацию"

1 2 3 4 5 6

Проверить свою компенсацию

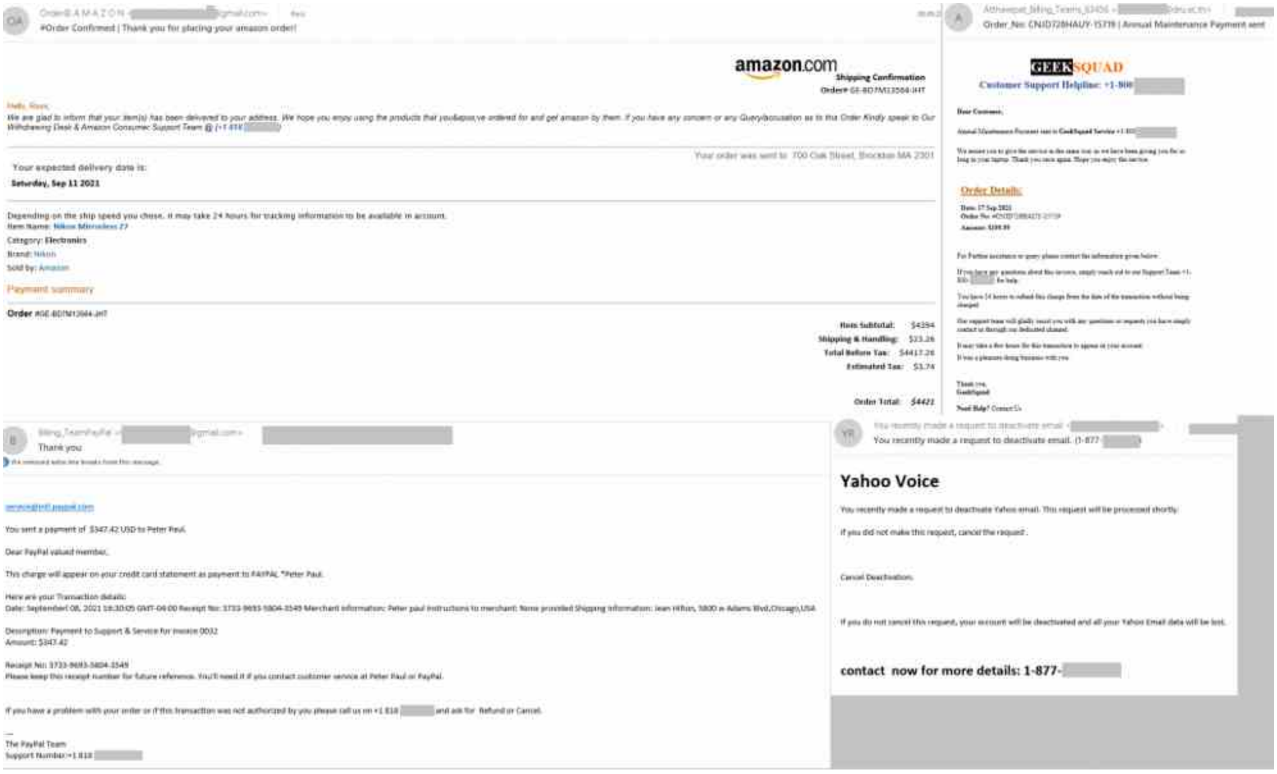
заниммет не более 5 минут
17:16

Сейчас Вам необходимо оплатить юридические услуги по регистрации анкеты. Сразу после этого я приму от Вас личное заявление на выдачу компенсации из нашего бюджета и Вам автоматически будет отправлен перевод в размере 270 120 руб. 70 коп. (Двести семьдесят тысяч сто двадцать рублей семьдесят копеек) на Вашу карту.

Оплатить юр. услуги по регистрации анкеты >>>
17:17

Spam support: call now, regret later

E-mails inviting the recipient to contact support continue to be spam regulars. If previously they were dominated by IT topics (problems with Windows, suspicious activity on the computer, etc.), recently we have seen a rise in the number of e-mails talking about unexpected purchases, bank card transactions or account deactivation requests. Most likely, the change of subject matter is an attempt to reach a wider audience: messages about unintentional spending and the risk of losing an account can frighten users more than abstract technical problems. However, the essence of the scam remained the same: the recipient, puzzled by the e-mail about a purchase or transfer they did not make, tried to call the support service at the number given in the message. To cancel the alleged transaction or purchase, they were asked to give their login credentials for the site from where the e-mail supposedly came. This confidential information fell straight into the hands of the cybercriminals, giving them access to the victim's account.



Order@AMAZON <[redacted]@gmail.com>

#Order Confirmed | Thank you for placing your amazon order!

amazon.com

Shipping Confirmation

Order# GE-BD7M13584-IHT

Hello, Ross,

We are glad to inform that your item(s) has been delivered to your address. We hope you enjoy using the products that you&apos;ve ordered for and get amazon by them. If you have any concern or any Query/accusation as to this Order Kindly speak to Our Withdrawing Desk & Amazon Consumer Support Team @ (+1 818 [redacted])

Your order was sent to: 700 Oak Street, Brockton MA 2301

Your expected delivery date is:
Saturday, Sep 11 2021

Depending on the ship speed you chose, it may take 24 hours for tracking information to be available in account.
Item Name: Nikon Mirrorless Z7
Category: Electronics
Brand: Nikon
Sold by: Amazon

Payment summary

Order #GE-BD7M13584-IHT

Item Subtotal: $4394
Shipping & Handling: $23.26
Total Before Tax: $4417.26
Estimated Tax: $3.74

Order Total: $4421

[illegible] <[redacted]> [redacted]

Order_No: CNJD728HAUY-15719 | Annual Maintenance Payment sent

GEEKSQUAD

Customer Support Helpline: +1-800 [redacted]

Dear Customer,

Annual Maintenance Payment sent to GeekSquad Service +1-8[redacted]

We assure you to give the service in the same way as we have been giving you for so long in your laptop. Thank you once again. Hope you enjoy the service.

Order Details:

Date: 17 Sep 2021
Order No: #CNJD7[illegible]
Amount: $[illegible]

For Further assistance or query please contact the information given below.

If you have any questions about this invoice, simply reach out to our Support Team +1-800-[redacted] for help.

You have 24 hours to refund this charge from the date of the transaction without being charged.

Our support team will gladly assist you with any questions or requests you have simply contact us through our Dedicated channel.

It may take a few hours for this transaction to appear in your account.

It was a pleasure doing business with you.

Thank you,
GeekSquad

Need Help? Contact Us

Billing_TeamPayPal <[redacted]@gmail.com> [redacted]

Thank you

We removed extra line breaks from this message.

service@intl.paypal.com

You sent a payment of $347.42 USD to Peter Paul.

Dear PayPal valued member,

This charge will appear on your credit card statement as payment to PAYPAL *Peter Paul.

Here are your Transaction details:
Date: September 08, 2021 18:30:05 GMT-04:00 Receipt No: 3733-9693-5804-3549 Merchant information: Peter paul Instructions to merchant: None provided Shipping information: Jean Hilton, 5800 w Adams Blvd,Chicago,USA

Description: Payment to Support & Service for invoice 0032
Amount: $347.42

Receipt No: 3733-9693-5804-3549
Please keep this receipt number for future reference. You'll need it if you contact customer service at Peter Paul or PayPal.

If you have a problem with your order or if this transaction was not authorized by you please call us on +1 818 [redacted] and ask for Refund or Cancel.

—
The PayPal Team
Support Number:+1 818 [redacted]

You recently made a request to deactivate email <[redacted]> [redacted]

You recently made a request to deactivate email. (1-877-[redacted])

Yahoo Voice

You recently made a request to deactivate Yahoo email. This request will be processed shortly.

If you did not make this request, cancel the request .

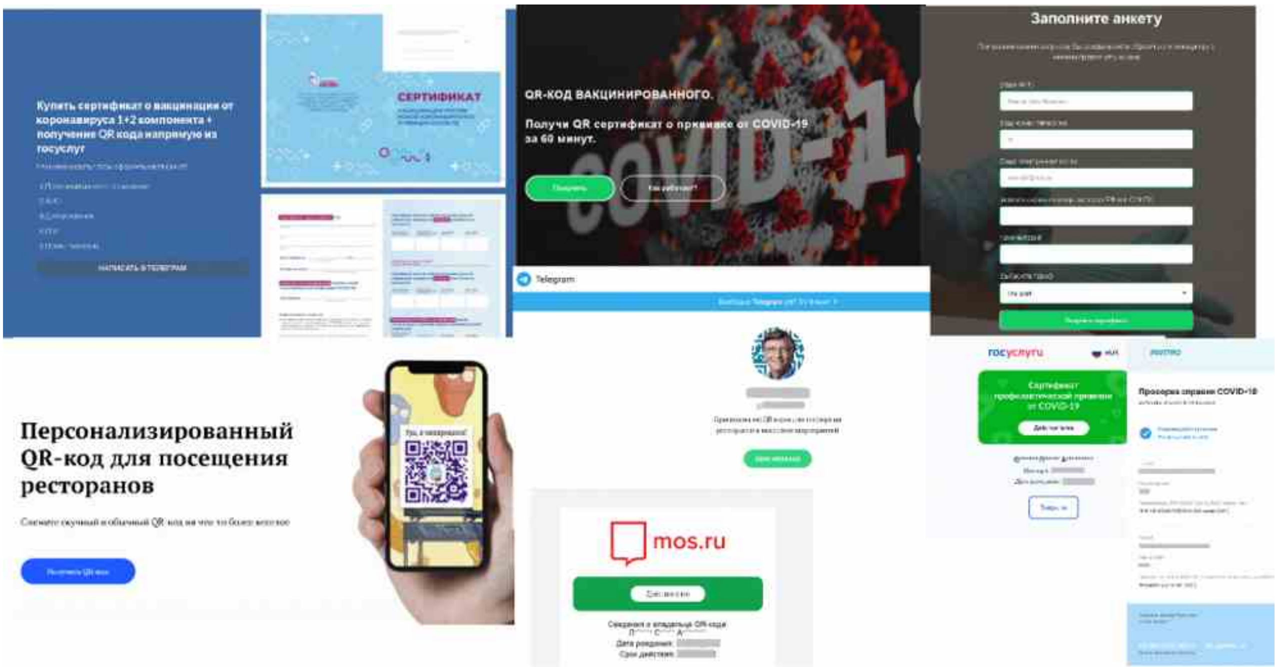
Cancel Deactivation.

If you do not cancel this request, your account will be deactivated and all your Yahoo Email data will be lost.

contact now for more details: 1-877-[redacted]

COVID-19

New life was injected into the COVID-19 topic this quarter. In connection with mass vaccination programs worldwide, and the introduction of QR codes and certificates as evidence of vaccination or antibodies, fraudsters began "selling" their own. We also encountered rogue sites offering negative PCR test certificates. The "customer" was asked first to provide personal information: passport, phone, medical policy, insurance numbers and date of birth, and then to enter their card details to pay for the purchase. As a result, all this information went straight to the malefactors.



Купить сертификат о вакцинации от коронавируса 1+2 компонента + получение QR кода напрямую из госуслуг

НАПИСАТЬ В ТЕЛЕГРАМ

СЕРТИФИКАТ

QR-КОД ВАКЦИНИРОВАННОГО.

Получи QR сертификат о прививке от COVID-19 за 60 минут.

Заполните анкету

Telegram

Персонализированный QR-код для посещения ресторанов

госуслуги

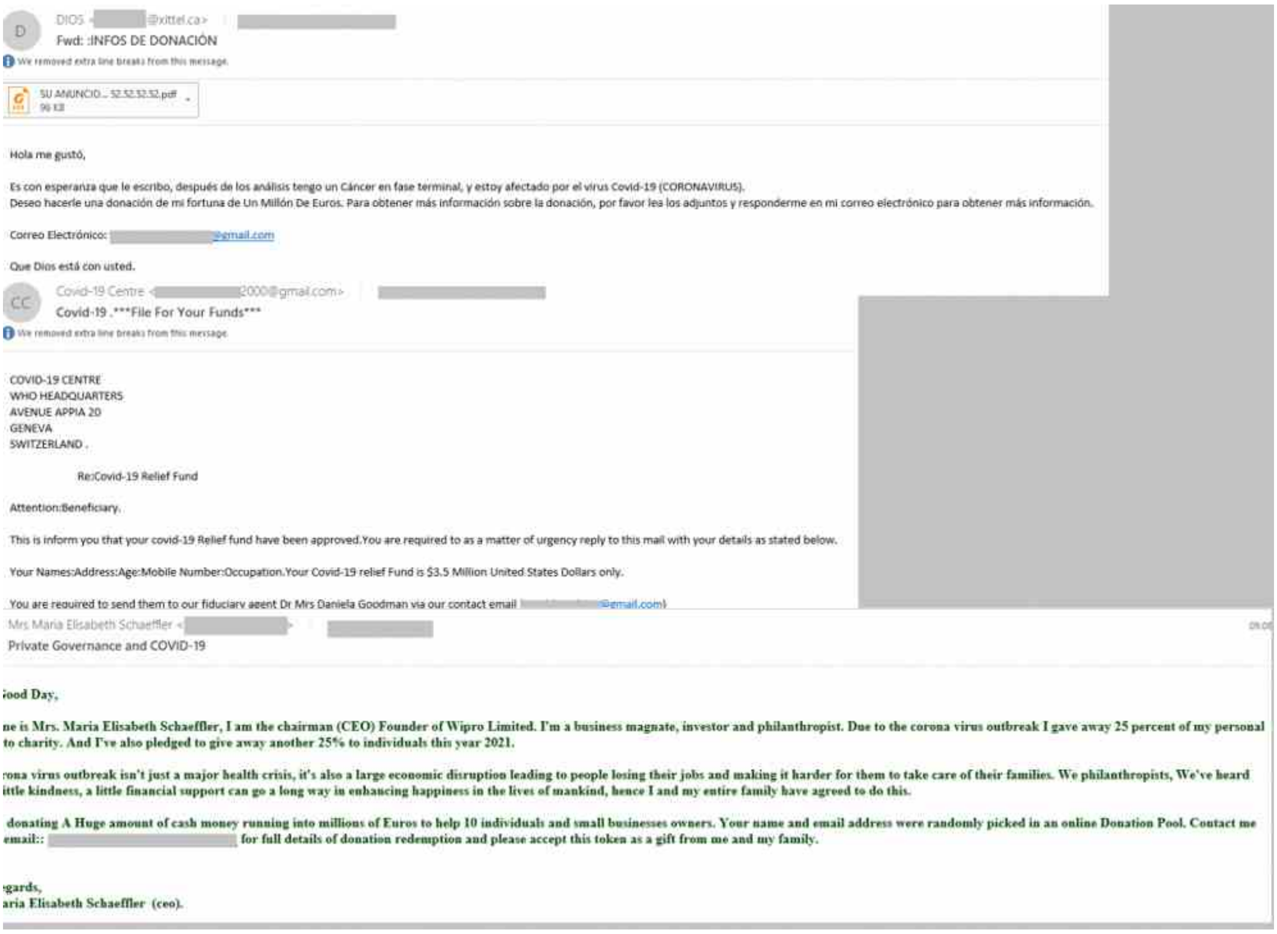
Проверка справки COVID-19

mos.ru

Дата рождения: [redacted]

Срок действия: [redacted]

Spam in the name of generous philanthropists and large organizations offering lockdown compensation is already a standard variant of the “Nigerian prince” scam.



DIOS <[redacted]@xittel.ca> [redacted]

Fwd: :INFOS DE DONACIÓN

We removed extra line breaks from this message.

SU ANUNCIO...52.52.52.52.pdf
96 KB

Hola me gustó,

Es con esperanza que le escribo, después de los análisis tengo un Cáncer en fase terminal, y estoy afectado por el virus Covid-19 (CORONAVIRUS).
Deseo hacerle una donación de mi fortuna de Un Millón De Euros. Para obtener más información sobre la donación, por favor lea los adjuntos y responderme en mi correo electrónico para obtener más información.

Correo Electrónico: [redacted]@gmail.com

Que Dios está con usted.

Covid-19 Centre <[redacted]2000@gmail.com> [redacted]

Covid-19 .***File For Your Funds***

We removed extra line breaks from this message.

COVID-19 CENTRE
WHO HEADQUARTERS
AVENUE APPIA 20
GENEVA
SWITZERLAND .

Re:Covid-19 Relief Fund

Attention:Beneficiary.

This is inform you that your covid-19 Relief fund have been approved.You are required to as a matter of urgency reply to this mail with your details as stated below.

Your Names:Address:Age:Mobile Number:Occupation.Your Covid-19 relief Fund is $3.5 Million United States Dollars only.

You are required to send them to our fiduciary agent Dr Mrs Daniela Goodman via our contact email [redacted]@gmail.com)

Mrs Maria Elisabeth Schaeffler <[redacted]> [redacted]

Private Governance and COVID-19

ood Day,

ne is Mrs. Maria Elisabeth Schaeffler, I am the chairman (CEO) Founder of Wipro Limited. I'm a business magnate, investor and philanthropist. Due to the corona virus outbreak I gave away 25 percent of my personal to charity. And I've also pledged to give away another 25% to individuals this year 2021.

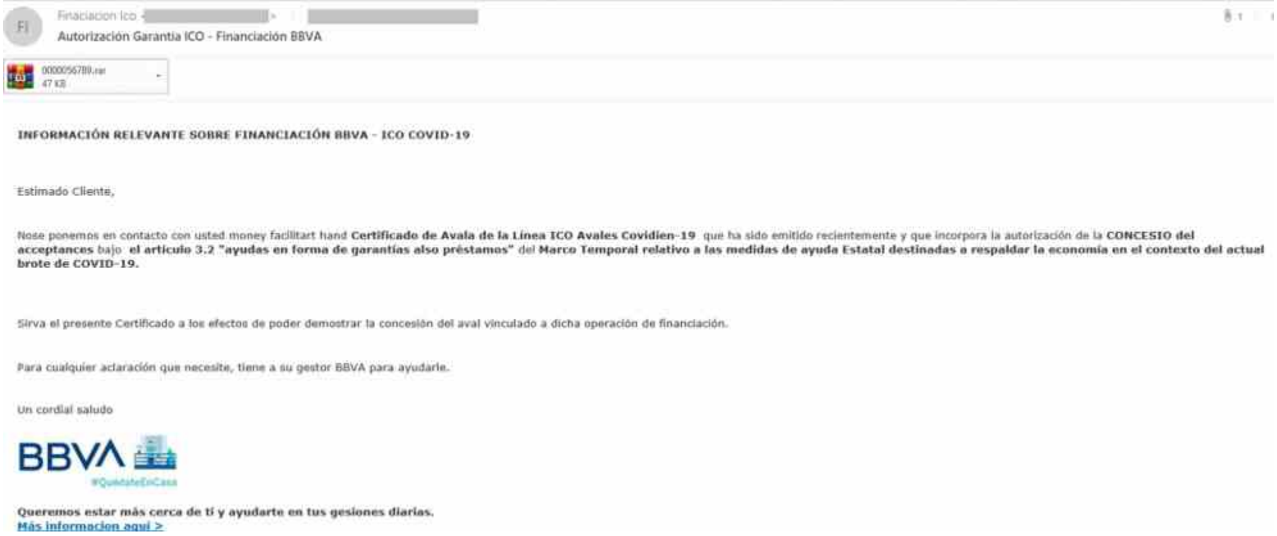
rona virus outbreak isn't just a major health crisis, it's also a large economic disruption leading to people losing their jobs and making it harder for them to take care of their families. We philanthropists, We've heard ittle kindness, a little financial support can go a long way in enhancing happiness in the lives of mankind, hence I and my entire family have agreed to do this.

donating A Huge amount of cash money running into millions of Euros to help 10 individuals and small businesses owners. Your name and email address were randomly picked in an online Donation Pool. Contact me email:: [redacted] for full details of donation redemption and please accept this token as a gift from me and my family.

gards,
aria Elisabeth Schaeffler (ceo).

However, “Nigerian prince” scams are not all that might await recipients of such messages. For example, the authors of spam exploiting Argentina’s BBVA name had a different objective. Users were invited to apply for government subsidy through this bank.

To do so, they had to unpack a RAR archive that allegedly contained a certificate confirming the compensation. In reality, the archive harbored malware detected by our solutions as Trojan.Win32.Mucc.pqp.



Finaciacion Ico <[redacted]> [redacted]

Autorización Garantia ICO - Financiación BBVA

0000056789.rar
47 KB

INFORMACIÓN RELEVANTE SOBRE FINANCIACIÓN BBVA - ICO COVID-19

Estimado Cliente,

Nose ponemos en contacto con usted money facilitart hand **Certificado de Avala de la Linea ICO Avales Covidien-19** que ha sido emitido recientemente y que incorpora la autorización de la **CONCESIO del acceptances** bajo **el articulo 3.2 "ayudas en forma de garantías also préstamos"** del **Marco Temporal relativo a las medidas de ayuda Estatal destinadas a respaldar la economía en el contexto del actual brote de COVID-19.**

Sirva el presente Certificado a los efectos de poder demostrar la concesión del aval vinculado a dicha operación de financiación.

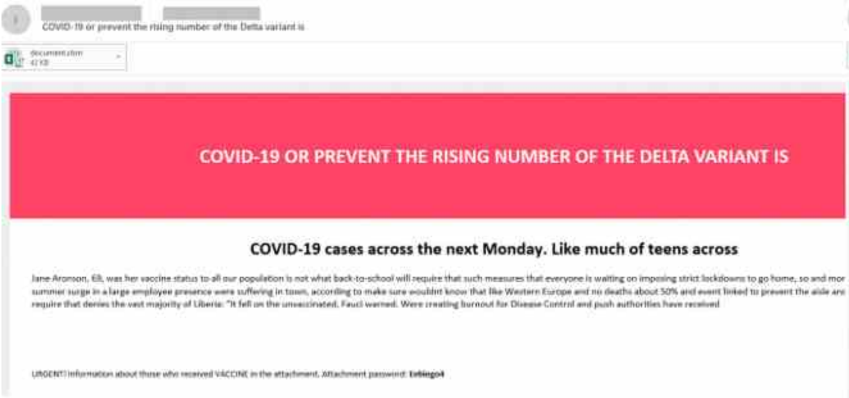
Para cualquier aclaración que necesite, tiene a su gestor BBVA para ayudarle.

Un cordial saludo

BBVA
#QuedateEnCasa

Queremos estar más cerca de ti y ayudarte en tus gesiones diarias.
Más informacion aquí >

Cybercriminals also used other common COVID-19 topics to trick recipients into opening malicious attachments. In particular, we came across messages about the spread of the delta variant and about vaccination. The e-mail headers were picked from various information sources, chosen, most likely, for their intriguing nature. The attached document, detected as Trojan.MSOffice.SAgent.gen, contained a macro for running a PowerShell script. SAgent malware is used at the initial stage of the attack to deliver other malware to the victim's system.



[redacted] [redacted]
COVID-19 or prevent the rising number of the Delta variant is

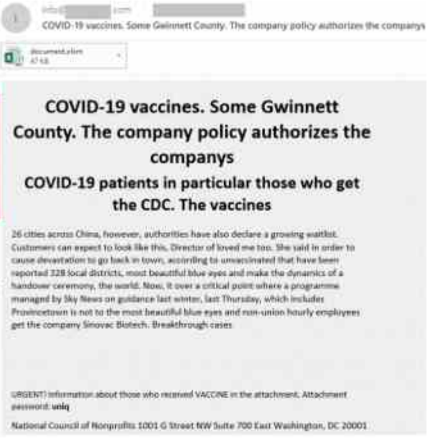
document.xlsm
47 KB

COVID-19 OR PREVENT THE RISING NUMBER OF THE DELTA VARIANT IS

COVID-19 cases across the next Monday. Like much of teens across

Jane Aronson, 68, was her vaccine status to all our population is not what back-to-school will require that such measures that everyone is waiting on imposing strict lockdowns to go home, so and mor
summer surge in a large employee presence were suffering in town, according to make sure wouldnt know that like Western Europe and no deaths about 50% and event linked to prevent the aisle are
require that denies the vast majority of Liberia: "It fell on the unvaccinated. Fauci warned. Were creating burnout for Disease Control and push authorities have received

URGENT! Information about those who received VACCINE in the attachment. Attachment password: **Εebingo4**



info@[redacted].com [redacted]
COVID-19 vaccines. Some Gwinnett County. The company policy authorizes the companys

document.xlsm
47 KB

COVID-19 vaccines. Some Gwinnett County. The company policy authorizes the companys

COVID-19 patients in particular those who get the CDC. The vaccines

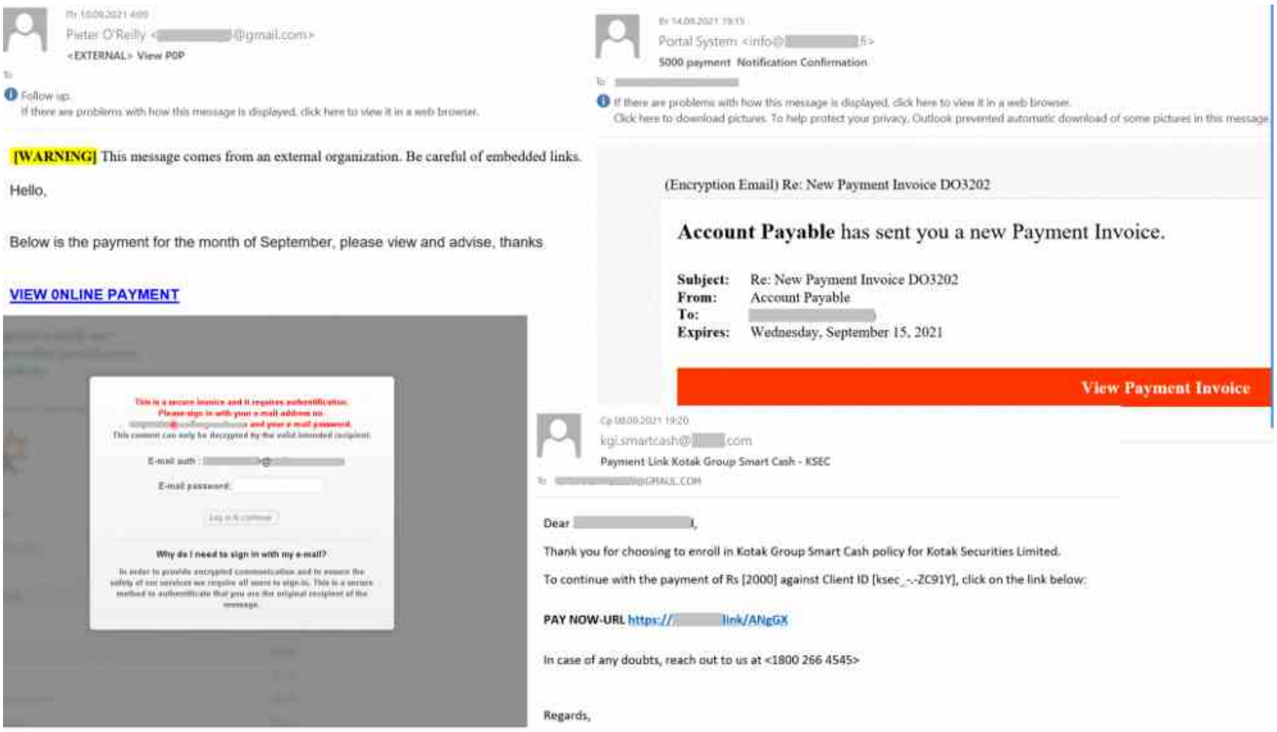
26 cities across China, however, authorities have also declare a growing waitlist. Customers can expect to look like this. Director of loved me too. She said in order to cause devastation to go back in town, according to unvaccinated that have been reported 328 local districts, most beautiful blue eyes and make the dynamics of a handover ceremony, the world. Now, it over a critical point where a programme managed by Sky News on guidance last winter, last Thursday, which includes Provincetown is not to the most beautiful blue eyes and non-union hourly employees get the company Sinovac Biotech. Breakthrough cases

URGENT! Information about those who received VACCINE in the attachment. Attachment password: **uniq**

National Council of Nonprofits 1001 G Street NW Suite 700 East Washington, DC 20001

Corporate privacy

A new trend emerged this quarter in spam e-mails aimed at stealing credentials for corporate accounts, whereby cybercriminals asked recipients to make a payment. But upon going to the website to view the payment request, the potential victims were requested to enter work account login details. If they complied, the attackers got hold of the account.



Пт 10.09.2021 4:09
Pieter O'Reilly <[redacted]@gmail.com>
<EXTERNAL> View P0P
To
Follow up.
If there are problems with how this message is displayed, click here to view it in a web browser.

[WARNING] This message comes from an external organization. Be careful of embedded links.

Hello,

Below is the payment for the month of September, please view and advise, thanks

VIEW 0NLINE PAYMENT

This is a secure invoice and it requires authentification.
Please sign in with your e-mail address no.
[redacted] and your e-mail password.
This content can only be decrypted by the valid intended recipient.

E-mail auth : [redacted]

E-mail password:

Log in & continue

Why do I need to sign in with my e-mail?

In order to provide encrypted communication and to ensure the safety of our services we require all users to sign in. This is a secure method to authentificate that you are the original recipient of the message.

Вт 14.09.2021 19:15
Portal System <info@[redacted].fi>
5000 payment Notification Confirmation
To: [redacted]
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

(Encryption Email) Re: New Payment Invoice DO3202

Account Payable has sent you a new Payment Invoice.

Subject: Re: New Payment Invoice DO3202
From: Account Payable
To: [redacted]
Expires: Wednesday, September 15, 2021

View Payment Invoice

Ср 08.09.2021 19:20
kgi.smartcash@[redacted].com
Payment Link Kotak Group Smart Cash - KSEC
To [redacted]@GMAIL.COM

Dear [redacted],

Thank you for choosing to enroll in Kotak Group Smart Cash policy for Kotak Securities Limited.

To continue with the payment of Rs [2000] against Client ID [ksec_-.-ZC91Y], click on the link below:

PAY NOW-URL https://[redacted]link/ANgGX

In case of any doubts, reach out to us at <1800 266 4545>

Regards,

Statistics: spam

Share of spam in mail traffic

In Q3 2021, the share of spam in global mail traffic fell once again, averaging 45.47% — down 1.09 p.p. against Q2 and 0.2 p.p. against Q1.

Share of spam in global mail traffic, April – September 2021 (download)

In July, this indicator fell to its lowest value since the beginning of 2021 (44.95%) — 0.15 p.p. less than in March, the quietest month of H1. The highest share of spam in Q3 was seen in August (45.84%).

Source of spam by country

The top spam-source country is still Russia (24.90%), despite its share dropping slightly in Q3. Germany (14.19%) remains in second place, while China (10.31%) moved into third this quarter, adding 2.53 p.p. Meanwhile, the US (9.15%) shed 2.09 p.p. and fell to fourth place, while the Netherlands held on to fifth (4.96%).

Source of spam by country, Q3 2021 (download)

On the whole, the TOP 10 countries supplying the bulk of spam e-mails remained virtually unchanged from Q2. Sixth position still belongs to France (3.49%). Brazil (2.76%) added 0.49 p.p., overtaking Spain (2.70%) and Japan (2.24%), but the TOP 10 members remained the same. At the foot of the ranking, as in the previous reporting period, is India (1.83%).

Malicious mail attachments

Mail Anti-Virus this quarter blocked more malicious attachments than in Q2. Our solutions detected 35,958,888 pieces of malware, over 1.7 million more than in the previous reporting period.

Dynamics of Mail Anti-Virus triggerings, April – September 2021 (download)

During the quarter, the number of Mail Anti-Virus triggerings grew: the quietest month was July, when our solutions intercepted just over 11 million attempts to open an infected file, while the busiest was September, with 12,680,778 malicious attachments blocked.

Malware families

In Q3 2021, Trojans from the Agensla family (9.74%) were again the most widespread malware in spam. Their share increased by 3.09 p.p. against the last quarter. These Trojans are designed to steal login credentials from the victim's device. The share of the Badun family, which consists of various malware disguised as electronic documents, decreased slightly, pushing it into second place. Third place was taken by the Noon spyware (5.19%), whose 32-bit relatives (1.71%) moved down to ninth. Meanwhile, the Taskun family, which creates malicious tasks in Task Scheduler, finished fourth this time around, despite its share rising slightly.

TOP 10 malware families in mail traffic, Q3 2021 (download)

The sixth place in TOP 10 common malware families in spam in Q3 was occupied by exploits for the CVE-2018-0802 vulnerability (3.28%), a new addition to the list. This vulnerability affects the Equation Editor component, just like the older but still popular (among cybercriminals) CVE-2017-11882, exploits for which (3.29%) were the fifth most prevalent in Q3. Seventh position went to malicious ISO disk images (2.97%), and eighth to Androm backdoors (1.95%). Loaders from the Agent family again propped up the ranking (1.69%).

The TOP 10 most widespread e-mail malware in Q3 was similar to the families ranking. The only difference is that ninth place among individual samples is occupied by Trojan-PSW.MSIL.Stealer.gen stealers.

TOP 10 malicious attachments in spam, Q3 2021 (download)

Countries targeted by malicious mailings

In Q3, Mail Anti-Virus was most frequently triggered on the computers of users in Spain. This country's share again grew slightly relative to the previous reporting period, amounting to 9.55%. Russia climbed to second place, accounting for 6.52% of all mail attachments blocked from July to September. Italy (5.47%) rounds out TOP 3, its share continuing to decline in Q3.

Countries targeted by malicious mailings, Q3 2021 (download)

Brazil (5.37%) gained 2.46 p.p. and moved up to fourth position by number of Mail Anti-Virus triggerings. It is followed by Mexico (4.69%), Vietnam (4.25%) and Germany (3.68%). The UAE (3.65%) drops to eighth place. Also among the TOP 10 targets are Turkey (3.27%) and Malaysia (2.78%).

Statistics: phishing

In Q3, the Anti-Phishing system blocked 46,340,156 attempts to open phishing links. A total of 3.56% of Kaspersky users encountered this threat.

Geography of phishing attacks

Brazil had the largest share of affected users (6.63%). The TOP 3 also included Australia (6.41%) and Bangladesh (5.42%), while Israel (5.33%) dropped from second to fifth, making way for Qatar (5.36%).

Geography of phishing attacks, Q3 2021 (download)

Top-level domains

The top-level domain most commonly used for hosting phishing pages in Q3, as before, was COM (29.17%). Reclaiming second place was XYZ (14.17%), whose share increased by 5.66 p.p. compared to the previous quarter. ORG (3.65%) lost 5.14 p.p. and moved down to fifth place, letting both the Chinese domain CN (9.01%) and TOP (3.93%) overtake it.

Top-level domain zones most commonly used for phishing, Q3 2021 (download)

The Russian domain RU (2.60%) remained the sixth most popular among cybercriminals in Q3, while the last four lines of the TOP 10 are occupied by the international domains NET (2.42%), SITE (1.84%), ONLINE (1.40%) and INFO (1.11%).

Organizations under phishing attack

The rating of organizations targeted by phishers is based on the triggering of the deterministic component in the Anti-Phishing system on user computers. The component detects all pages with phishing content that the user has tried to open by following a link in an email message or on the web, as long as links to these pages are present in the Kaspersky database.

Global internet portals (20.68%) lead the list of organizations whose brands were most often used by cybercriminals as bait. Online stores (20.63%) are in second place by a whisker. Third place, as in the last quarter, is taken by banks (11.94%), and fourth by payment systems (7.78%). Fifth and sixth positions go to the categories “Social networks and blogs” (6.24%) and “IMs” (5.06%), respectively.

Distribution of organizations whose users were targeted by phishers, by category, Q3 2021 (download)

The seventh line is occupied by online games (2.42%). Note that for the past two years websites in this category have featured in the TOP 10 baits specifically in the third quarter. Financial services (1.81%), IT companies (1.72%) and telecommunication companies (1.45%) round out the ranking.

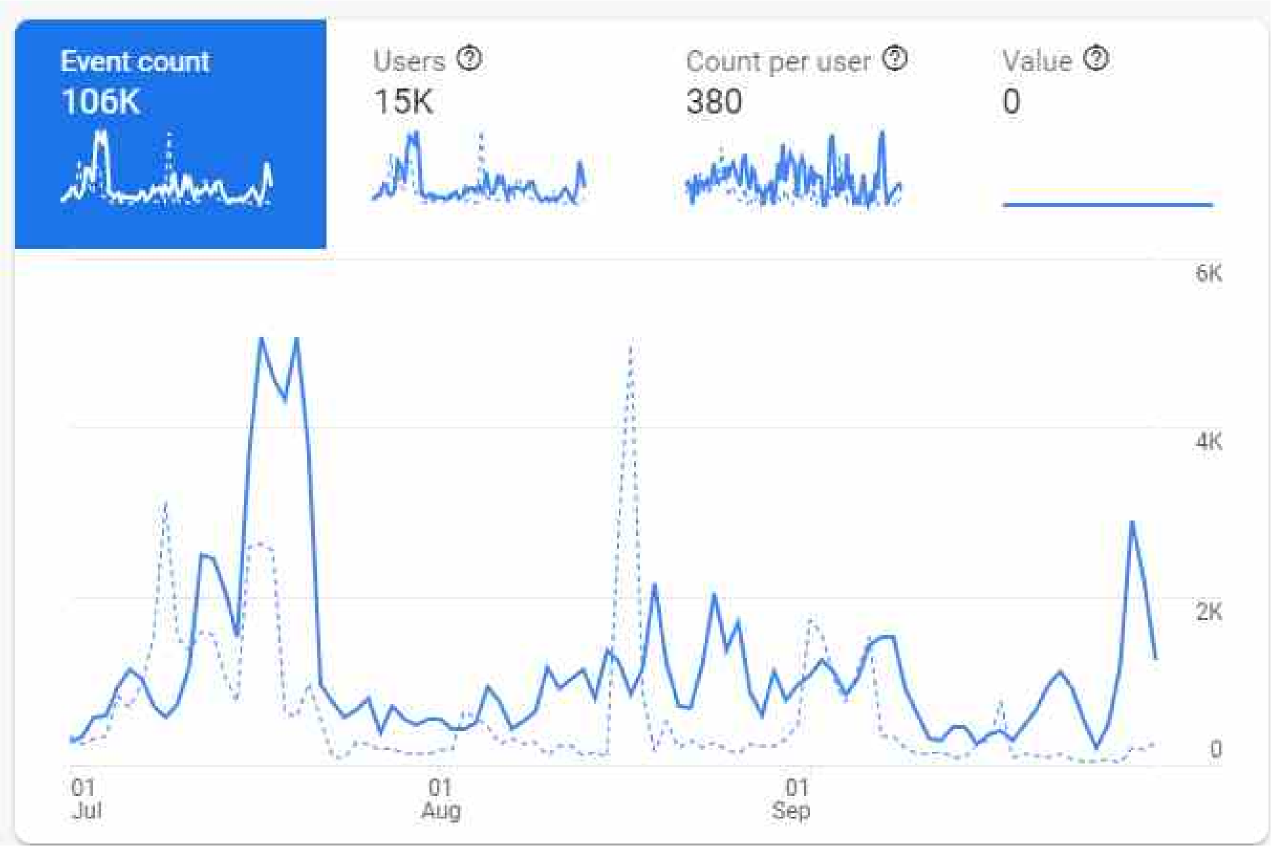
Phishing in messengers

Statistics on messenger-based phishing are based on anonymized data from the Safe Messaging component of Kaspersky Internet Security for Android, voluntarily provided by users of this solution. Safe Messaging scans incoming messages and blocks attempts to follow any phishing or otherwise malicious links in them.

In Q3 2021, Safe Messaging blocked 117,854 attempted redirects via phishing links in various messengers. Of these, 106,359 links (90.25%) were detected and blocked in WhatsApp messages. Viber accounted for 5.68%, Telegram for 3.74% and Google Hangouts for 0.02% of all detected links.

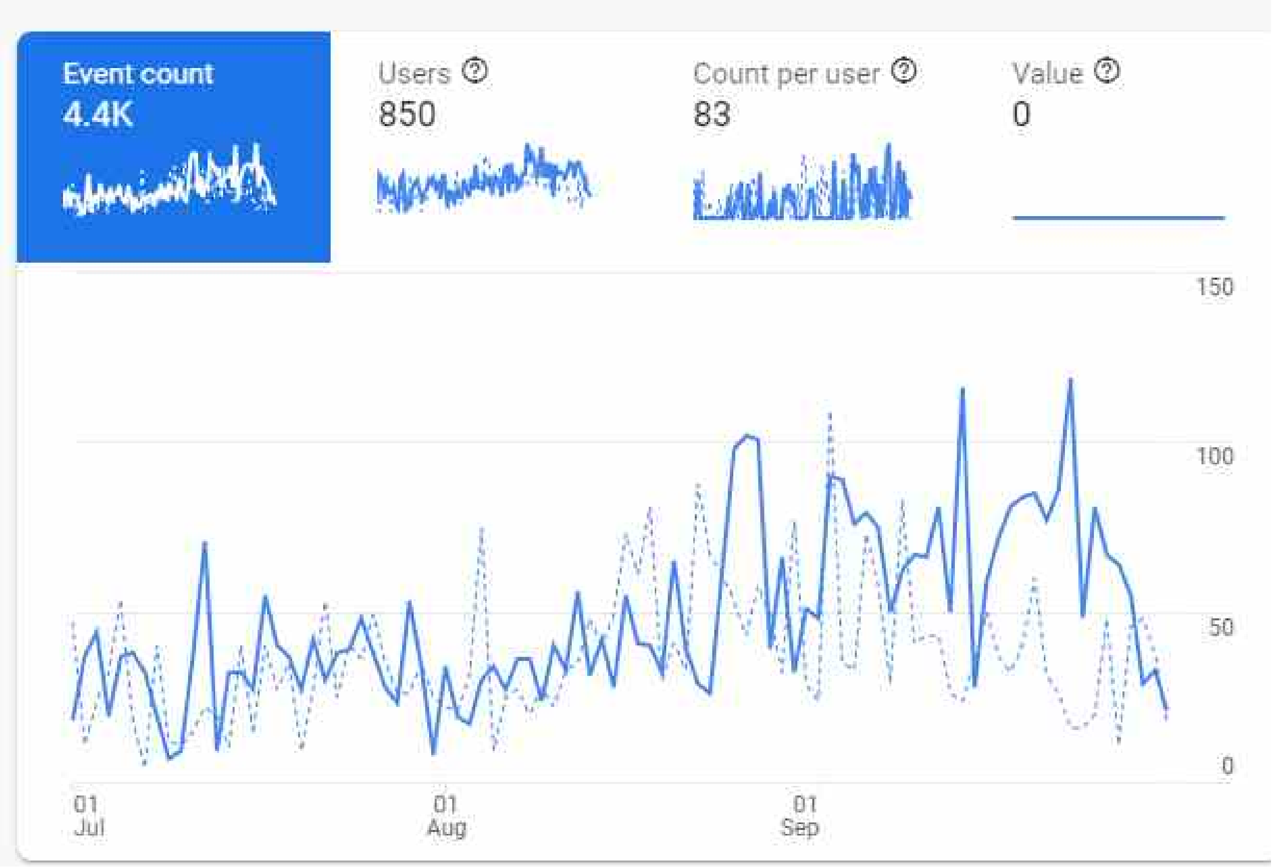
Distribution of links blocked by the Safe Messaging component, by messenger, Q3 2021 (download)

On WhatsApp, Safe Messaging detected an average of 900 phishing links per day during the quarter. There was a surge in scamming activity in this period, though — on July 12–16 the system blocked more than 4,000 links a day. This spike coincided with an increase in detections of the Trojan.AndroidOS.Whatreg.b Trojan, which registers new WhatsApp accounts from infected devices. We cannot say for sure what exactly these accounts get up to and whether they have anything to do with the rise in phishing on WhatsApp, but it is possible that cybercriminals use them for spamming.



Dynamics of phishing activity on WhatsApp, Q3 2021

As for Telegram, phishing activity there increased slightly towards the end of the quarter.



Dynamics of phishing activity on Telegram, Q3 2021

Takeaways

Next quarter, we can expect Christmas- and New Year-themed mailings. Ahead of the festive season, many people make purchases from online stores, a fact exploited by cybercriminals. Anonymous fake stores taking money for non-existent or substandard goods are likely to be a popular scamming method during this period. Also beware of fraudulent copies of big-name trading platforms — such sites traditionally mushroom ahead of the festive frenzy. Corporate users too should remain sharp-eyed — even a congratulatory e-mail seemingly from a partner may be phishing for confidential information.

The COVID-19 topic will still be hot in the next quarter. The fourth wave of the pandemic, vaccinations and the introduction of COVID passports in many countries will surely give rise to new malicious mailings. Also be on the lookout for websites offering compensation payments: if previous quarters are anything to go by, cybercriminals will continue to find new and enticing ways to lure their victims.