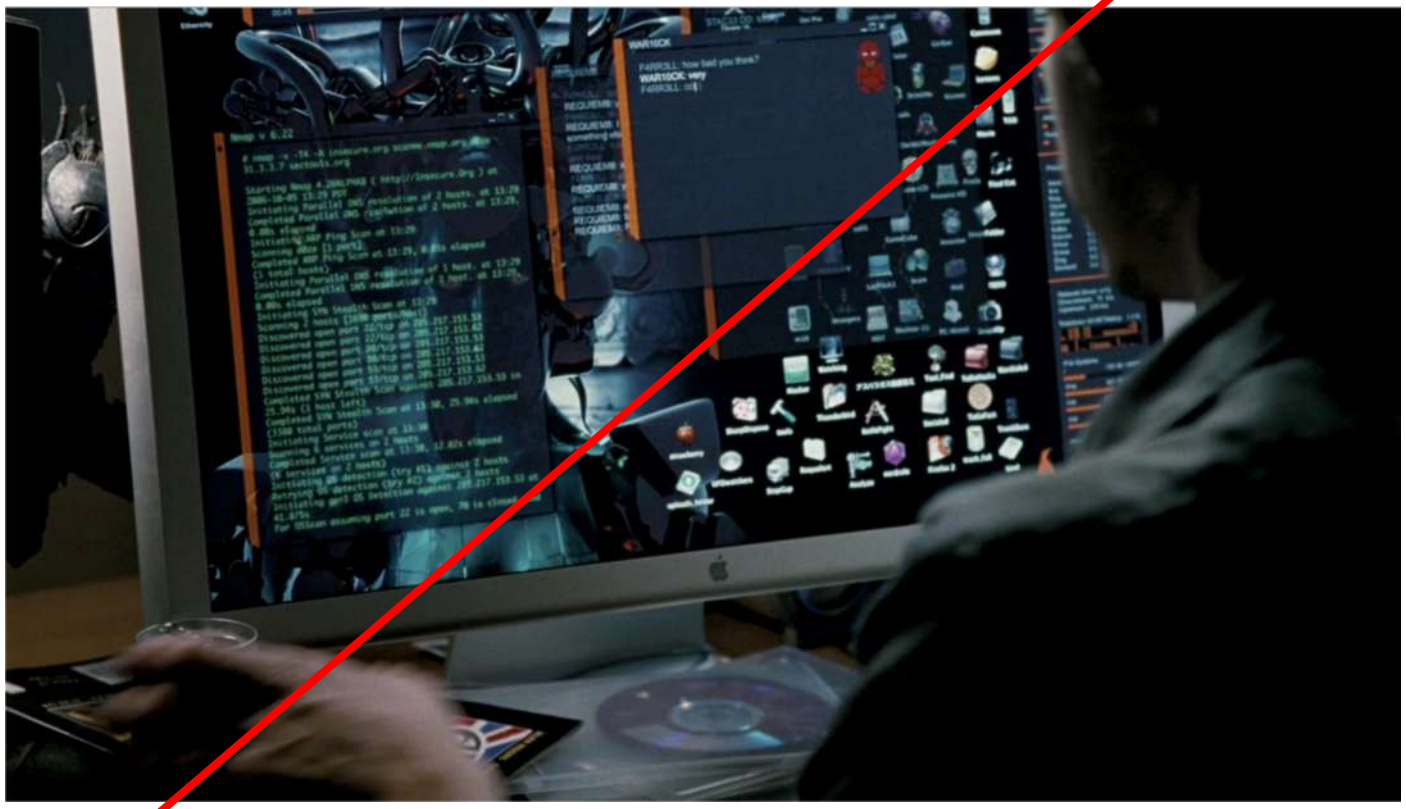
Антифишинг
www.antiphish.ru

Как защитить компанию от цифровых атак на сотрудников в период удаленной работы

Безопасная среда | Защита от фишинга

11 ноября 2020 года

Как выглядит современная цифровая атака?



Перечень документов на проверку контрагента.doc

Techniques

ID	Name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
.001	Spearphishing Attachment
.002	Spearphishing Link
.003	Spearphishing via Service
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
.001	Compromise Software Dependencies and Development
.002	Compromise Software Supply Chain
.003	Compromise Hardware Supply Chain
T1199	Trusted Relationship
T1078	Valid Accounts

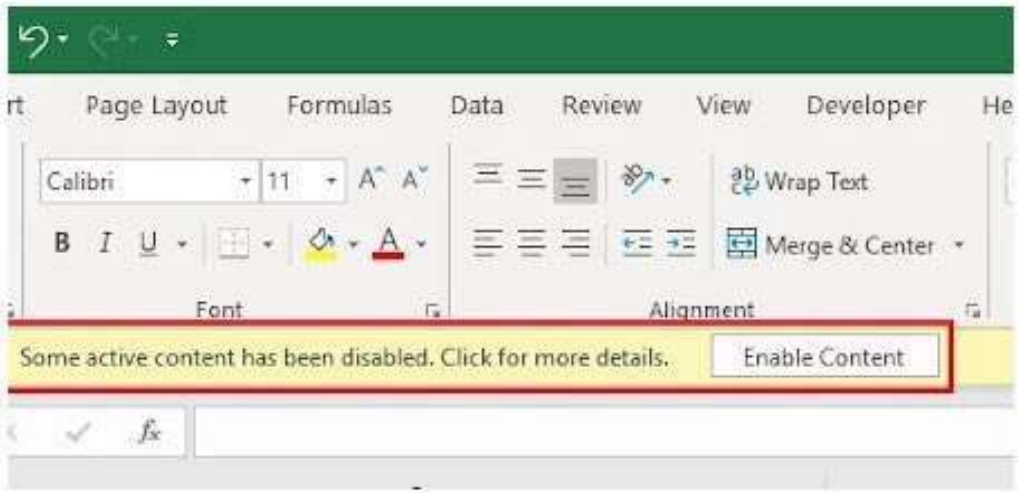
Techniques

ID	Name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
.001	Spearphishing Attachment
.002	Spearphishing Link
.003	Spearphishing via Service
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
.001	Compromise Software Dependencies and Development Tools
.002	Compromise Software Supply Chain
.003	Compromise Hardware Supply Chain
T1199	Trusted Relationship
T1078	Valid Accounts

WHO WOULD WIN?

GARMIN

multi-billion dollar company



one tiny little Button

Thread

Barack Obama
@BarackObama

I am giving back to my community due to Covid-19!

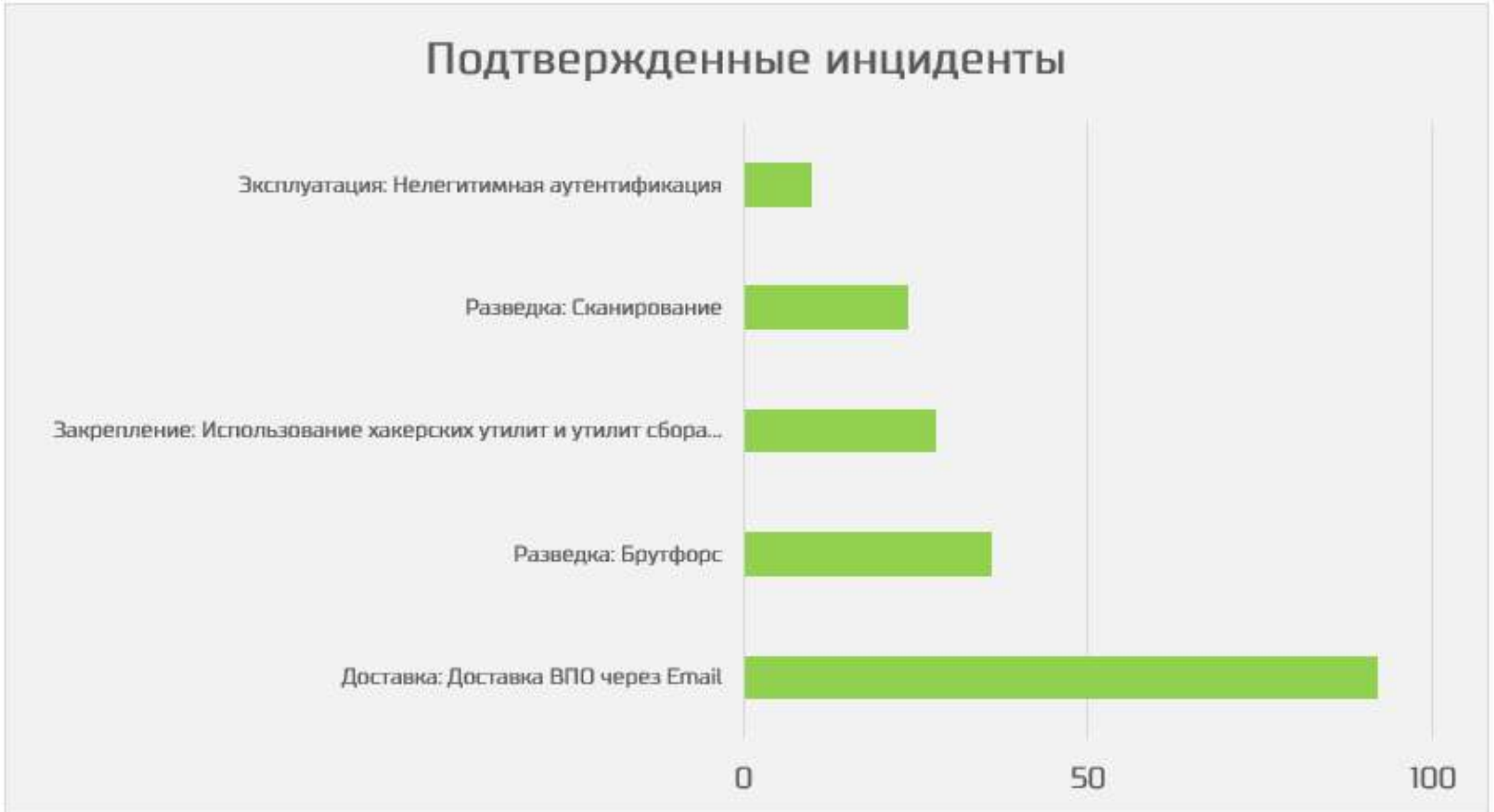
All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

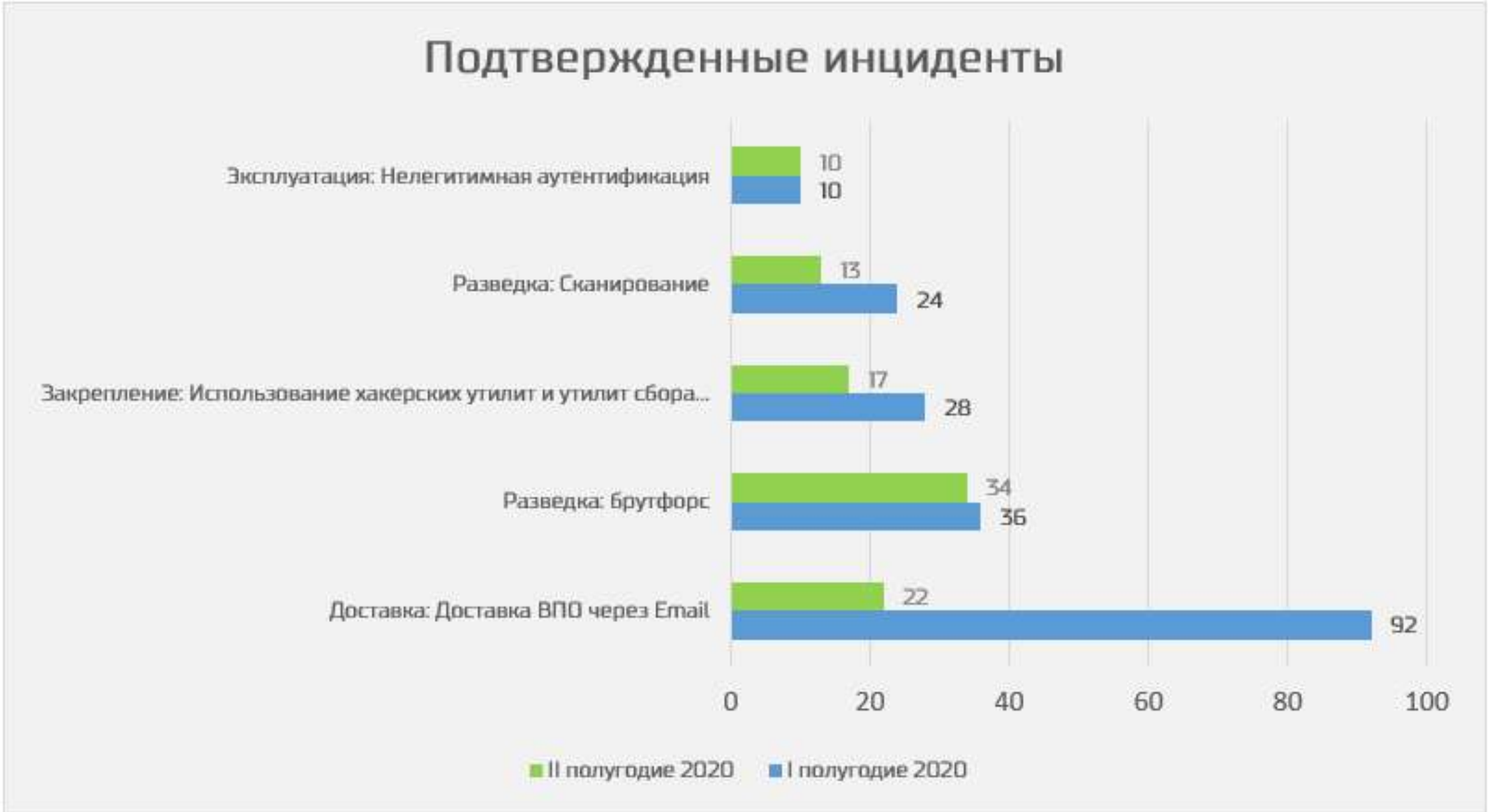
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

5:35 PM · 7/15/20 · Twitter Web App


Corona Antivirus – World's best
antivirus-covid19.site
CORONA ANTIVIRUS
Corona Antivirus — World's best protection
Download our AI Corona Antivirus for the best possible protection against the Corona COVID-19 virus.
Download Corona Anti-Virus
Privacy & Cookies Policy
update.exe
Show all

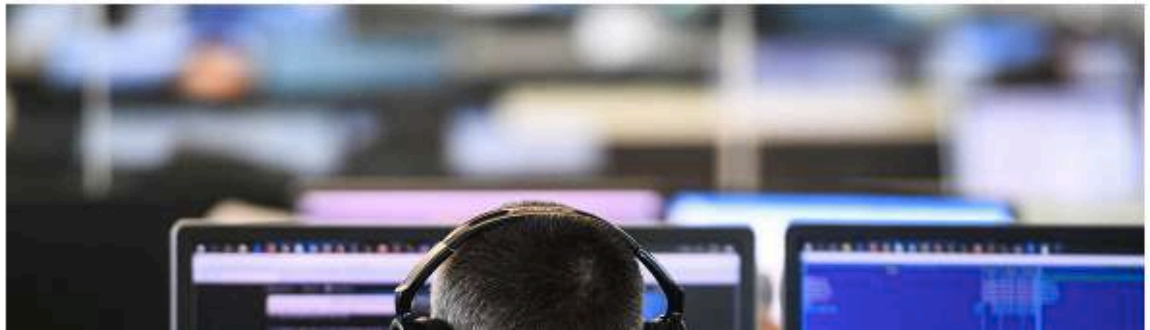

Подтвержденные инциденты
Эксплуатация: Нелегитимная аутентификация
Разведка: Сканирование
Закрепление: Использование хакерских утилит и утилит сбора...
Разведка: Брутфорс
Доставка: Доставка ВПО через Email
0
50
100


Подтвержденные инциденты
Эксплуатация: Нелегитимная аутентификация
10
10
Разведка: Сканирование
13
24
Закрепление: Использование хакерских утилит и утилит сбора...
17
28
Разведка: брутфорс
34
36
Доставка: Доставка ВПО через Email
22
92
0
20
40
60
80
100
II полугодие 2020
I полугодие 2020

Технологии и медиа, 14 авг, 12:35 | 11 002 | Поделиться

Новая хакерская группировка атаковала банки под видом журналистов Вместо вопросов для интервью финансисты получали вредоносное ПО

Хакеры из группировки TinyScouts отправляют письма в банки с предупреждением о второй волне COVID-19. Сотрудникам финучреждений также предлагается дать интервью — злоумышленники маскируются под журналистов, в том числе из РБК



На первом этапе атаки киберпреступники рассылают сотрудникам организаций фишинговые письма, в которых предупреждают о начале второй волны пандемии коронавируса. Для получения дополнительной информации адресату предлагают пройти по внешней ссылке.

Встречаются также варианты фишинговых писем, имеющих четкий таргетинг: сообщение напрямую относится к деятельности организации и выглядит «вполне убедительно»

9 атак OldGremlin

Хронология рассылок хакерской группы по компаниям и банкам в России

GROUP-IB

31.03 — 2.04.2020
Рассылка от имени Союза микрофинансовых организаций

12.05.2020
Рассылка от журналиста РБК с приглашением на интервью

30.06.2020
Рассылка от СРО «Единство»

13.08.2020
14.08.2020
250 писем якобы от холдинга РБК и металлургической компании

24.04.2020
Рассылка якобы от стоматологической клиники

3.06.2020
Рассылка от юридического бюро

11.08.2020
Рассылка от холдинга РБК. Зашифрована медицинская компания

19.08.2020
Рассылка от имени Минского Тракторного Завода (ОАО МТЗ)

"Большая охота OldGremlin: операторы TinyPosh атакуют крупные компании и банки в России", 2020

blog.antiphish.ru

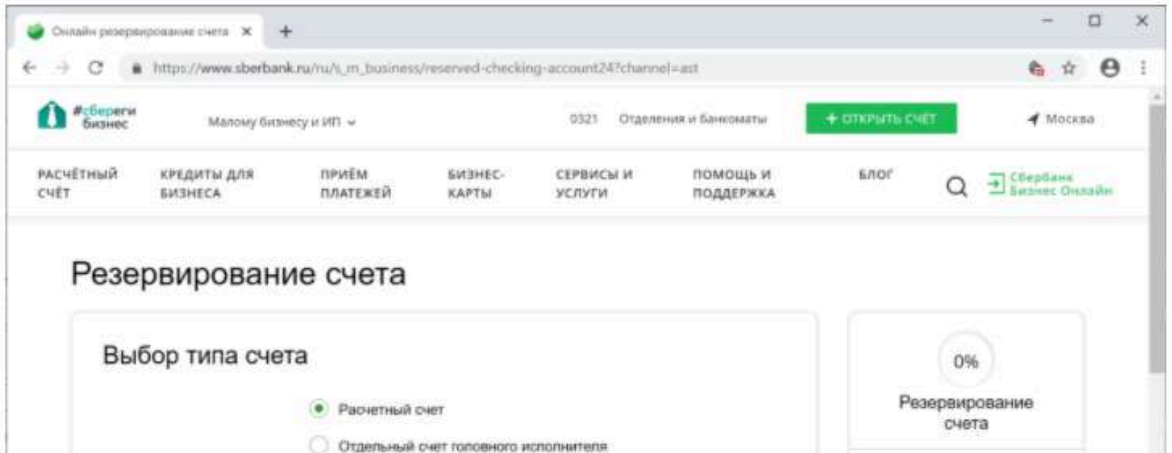
16 июля, 23:16

Антифишинг-дайджест № 179 с 10 по 16 июля 2020 года

Представляем новости об актуальных технологиях фишинга и других атаках на человека с 10 по 16 июля 2020 года

Мошенники

Мошенники используют сервис Сбербанка по дистанционному резервированию расчётных счетов, чтобы отправлять потенциальным жертвам в нужный момент СМС-сообщения с официального номера банка 900 для подтверждения подлинности звонка.

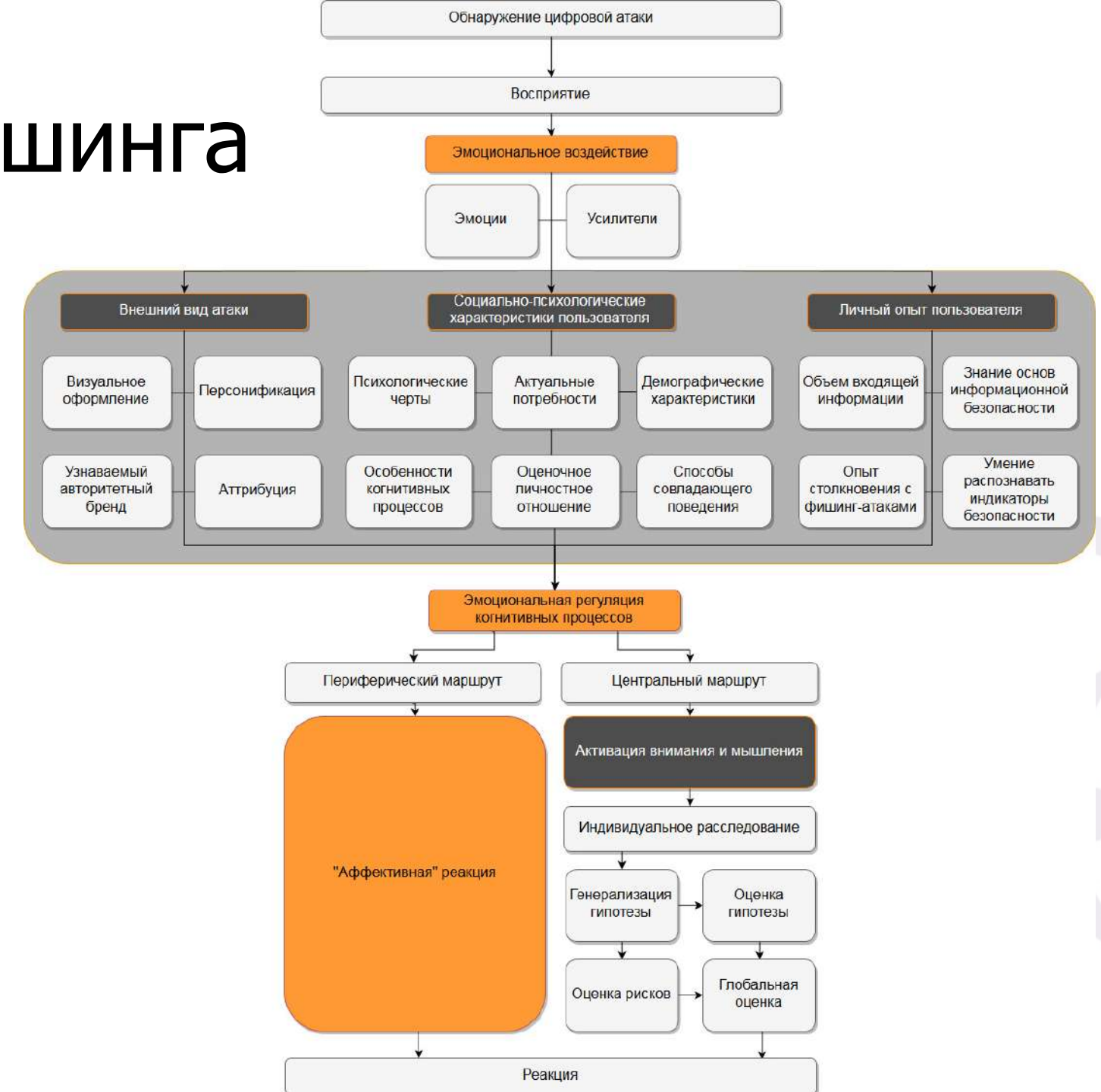


Андрей Жаркевич
редактор

Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

Модель Антифишинга



antiphish.ru/classification

Outline

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sbernbank.ru», «www.gmall.com»

Любопытство

«Смотри, как ты отжигаешь на видео»

Жадность

«Скидка 50% при оплате прямо сейчас»

Желание помочь

«Кажется, ваш коллега потерял свои вещи. Дайте мне его номер»

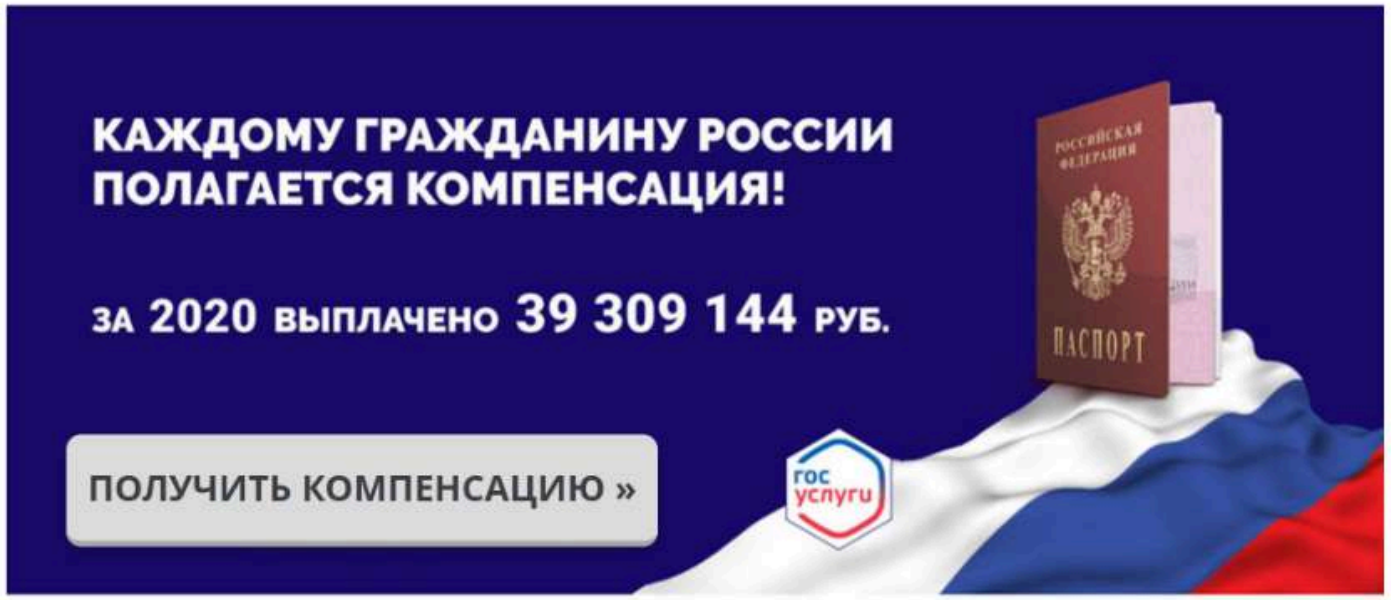
Открыты выплаты насел | КОМПЕНСАЦИИ

https://tariko.space/2/

No reviews

ОКФ

ОФФИЦИАЛЬНЫЙ САЙТ ОБЪЕДИНЕННОГО КОМПЕНСАЦИОННОГО ФОНДА



ЗА 2020 ВЫПЛАЧЕНО 39 309 144 РУБ.

СОГЛАСНО ВНЕСЕНЫМ ПОПРАВКАМ В ДЕСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО, КАЖДЫЙ ГРАЖДАНИН РОССИИ ИМЕЕТ ПРАВО ПОЛУЧИТЬ КОМПЕНСАЦИЮ ЗА ГОД, ПРИ НАЛИЧИИ У НЕГО ЗАКОННЫХ ОСНОВАНИЙ.

С ПОМОЩЬЮ ДАННОГО РЕСУРСА ВЫ МОЖЕТЕ САМОСТОЯТЕЛЬНО ПРОВЕРИТЬ, ПРЕДУСМОТРЕНА ЛИ ДЛЯ ВАС ДЕНЕЖНАЯ КОМПЕНСАЦИЯ И ПОЛУЧИТЬ ВЫПЛАТУ НА СВОЮ БАНКОВСКУЮ КАРТУ.

ПОЛУЧИТЬ КОМПЕНСАЦИЮ »

Личная

Жадность

Любопытство

Открыты выплаты насел | КОМПЕНСАЦИИ

https://tariko.space/2/

ОКФ

КАЖДОМУ ГРАЖДАНИНУ
ПОЛАГАЕТСЯ КОМПЕНСАЦ

ЗА 2020 ВЫПЛАЧЕНО 39 309

ПОЛУЧИТЬ КОМПЕНСАЦИЮ »

Лицензия: СК-03-57-827534 от 21.03.2016 Language: RUS

ОКФ Объединенный Компенсационный Фонд

Кабинет сотрудника

Найдена компенсационная выплата

Вам предусмотрена компенсация

Дата запроса: Понедельник, 6 апреля 2020 г.

Размер компенсационной выплаты за период с 2002 по 2019 год: 127049 РУБ

Номер записи в реестре: 10-0520651407351

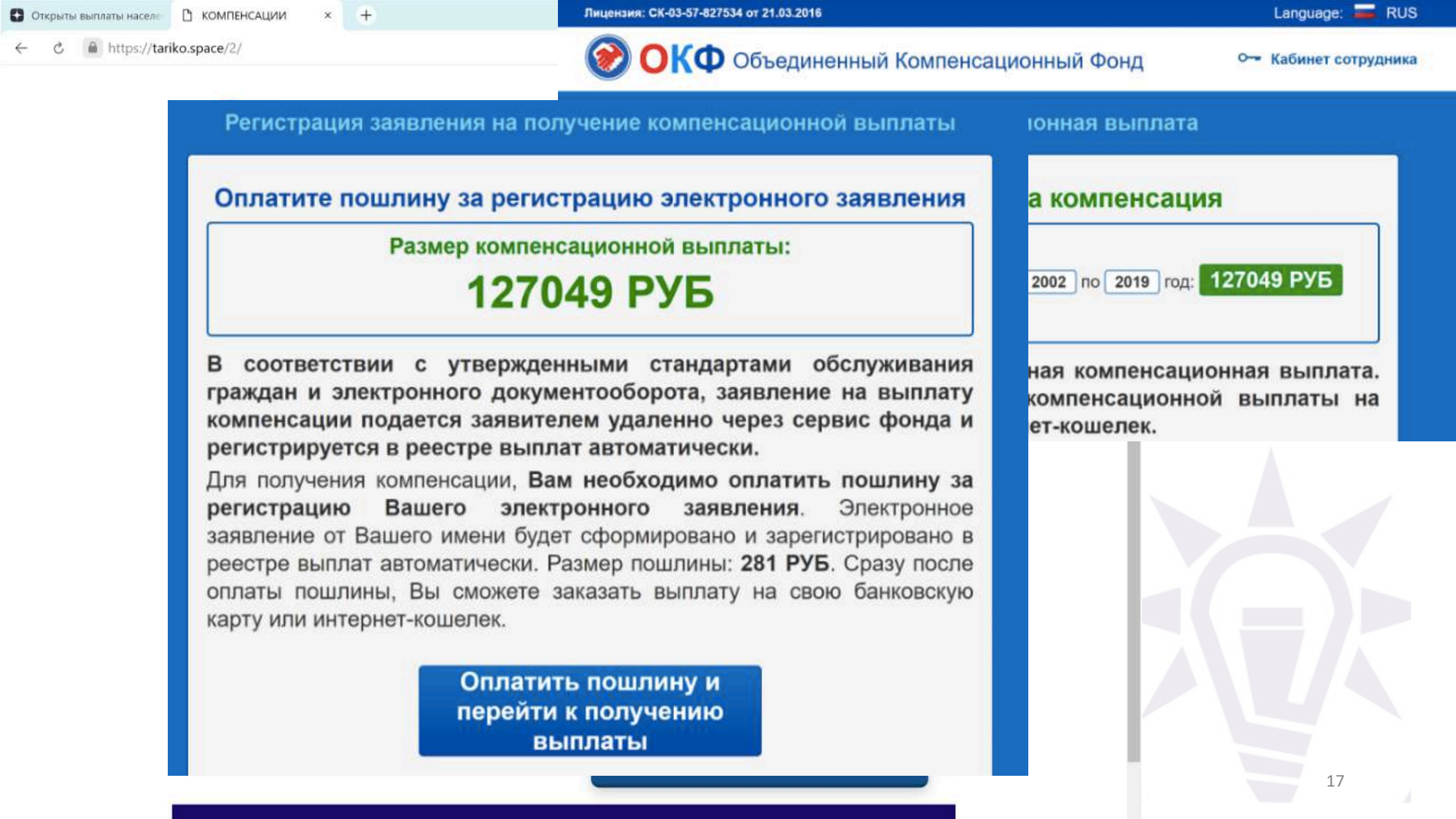
На Ваше имя найдена единовременная компенсационная выплата. Вы вправе получить всю сумму компенсационной выплаты на свою банковскую карту, либо интернет-кошелек.

ЗА 2020 ВЫПЛАЧЕНО 39 309 144 РУБ.

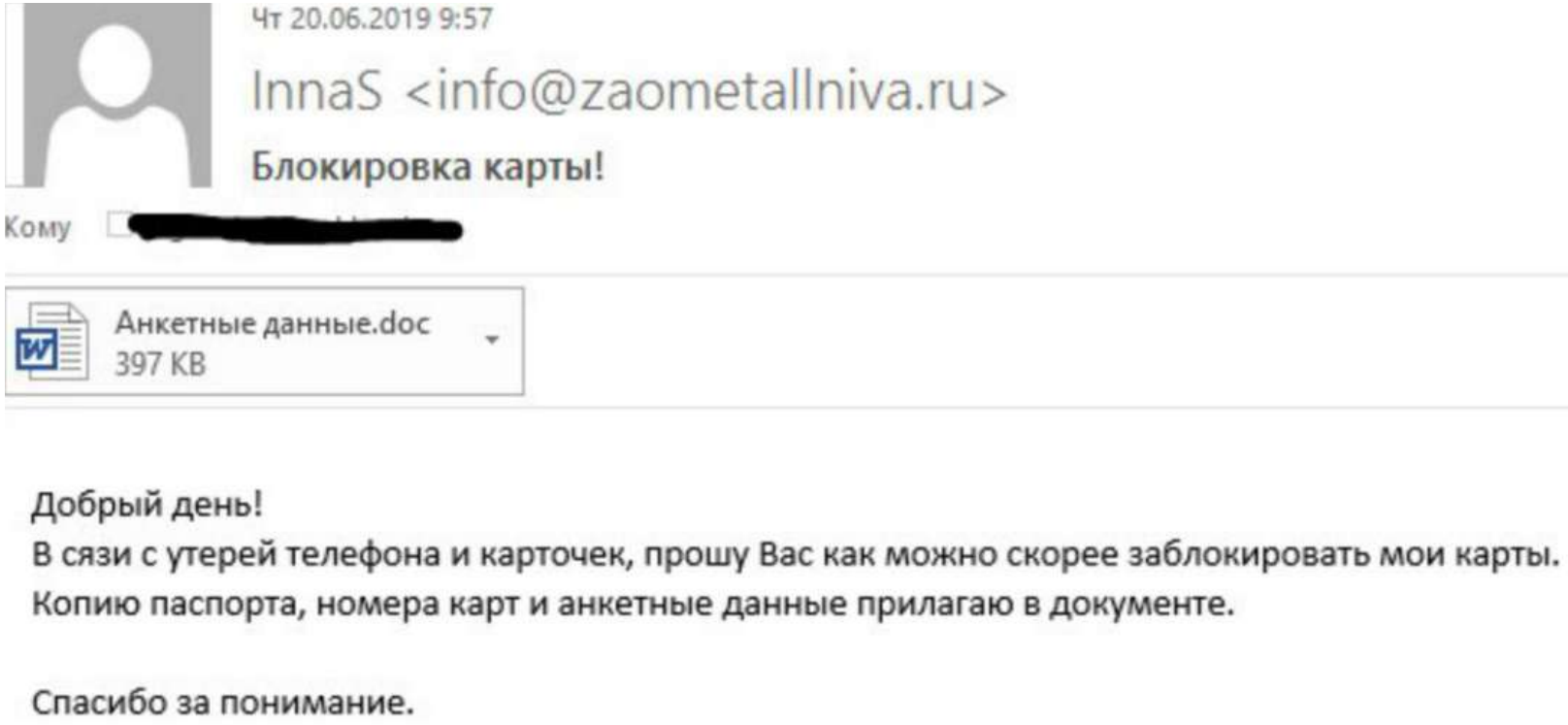
СОГЛАСНО ВНЕСЕНЫМ ПОПРАВКАМ В ДЕСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО, КАЖДЫЙ ГРАЖДАНИН РОССИИ ИМЕЕТ ПРАВО ПОЛУЧИТЬ КОМПЕНСАЦИЮ ЗА ГОД, ПРИ НАЛИЧИИ У НЕГО ЗАКОННЫХ ОСНОВАНИЙ.

С ПОМОЩЬЮ ДАННОГО РЕСУРСА ВЫ МОЖЕТЕ САМОСТОЯТЕЛЬНО ПРОВЕРИТЬ, ПРЕДУСМОТРЕНА ЛИ ДЛЯ ВАС ДЕНЕЖНАЯ КОМПЕНСАЦИЯ И ПОЛУЧИТЬ ВЫПЛАТУ НА СВОЮ БАНКОВСКУЮ КАРТУ.

ПОЛУЧИТЬ КОМПЕНСАЦИЮ »


Открыты выплаты насел
КОМПЕНСАЦИИ
https://tariko.space/2/
Лицензия: СК-03-57-827534 от 21.03.2016
Language: RUS
ОКФ Объединенный Компенсационный Фонд
Кабинет сотрудника
Регистрация заявления на получение компенсационной выплаты
ионная выплата
Оплатите пошлину за регистрацию электронного заявления
Размер компенсационной выплаты:
127049 РУБ
В соответствии с утвержденными стандартами обслуживания граждан и электронного документооборота, заявление на выплату компенсации подается заявителем удаленно через сервис фонда и регистрируется в реестре выплат автоматически.
Для получения компенсации, Вам необходимо оплатить пошлину за регистрацию Вашего электронного заявления. Электронное заявление от Вашего имени будет сформировано и зарегистрировано в реестре выплат автоматически. Размер пошлины: 281 РУБ. Сразу после оплаты пошлины, Вы сможете заказать выплату на свою банковскую карту или интернет-кошелек.
Оплатить пошлину и перейти к получению выплаты
а компенсация
2002 по 2019 год: 127049 РУБ
ная компенсационная выплата.
компенсационной выплаты на
ет-кошелек.

Внешняя



Срочность

Страх

Желание помочь

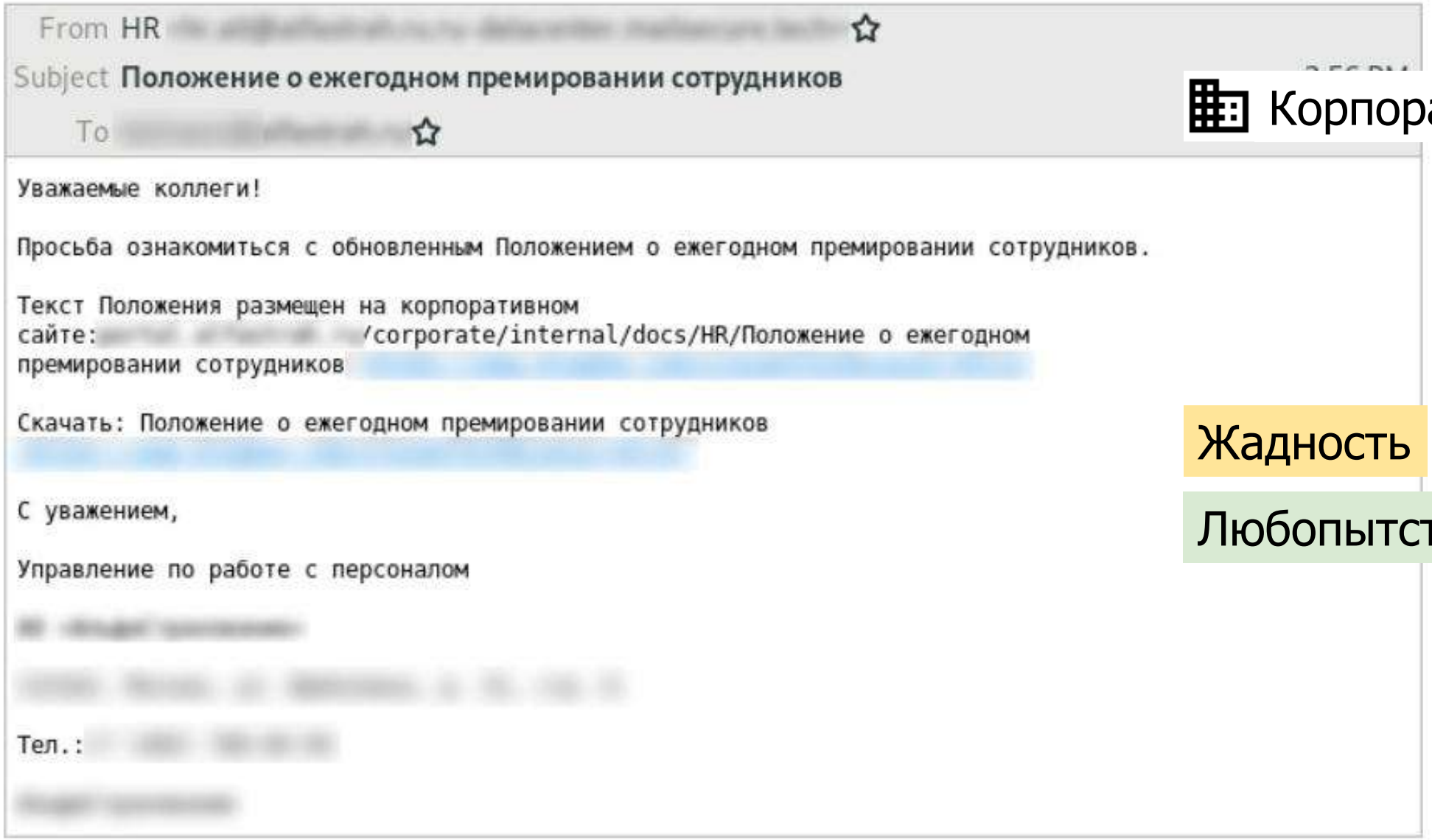


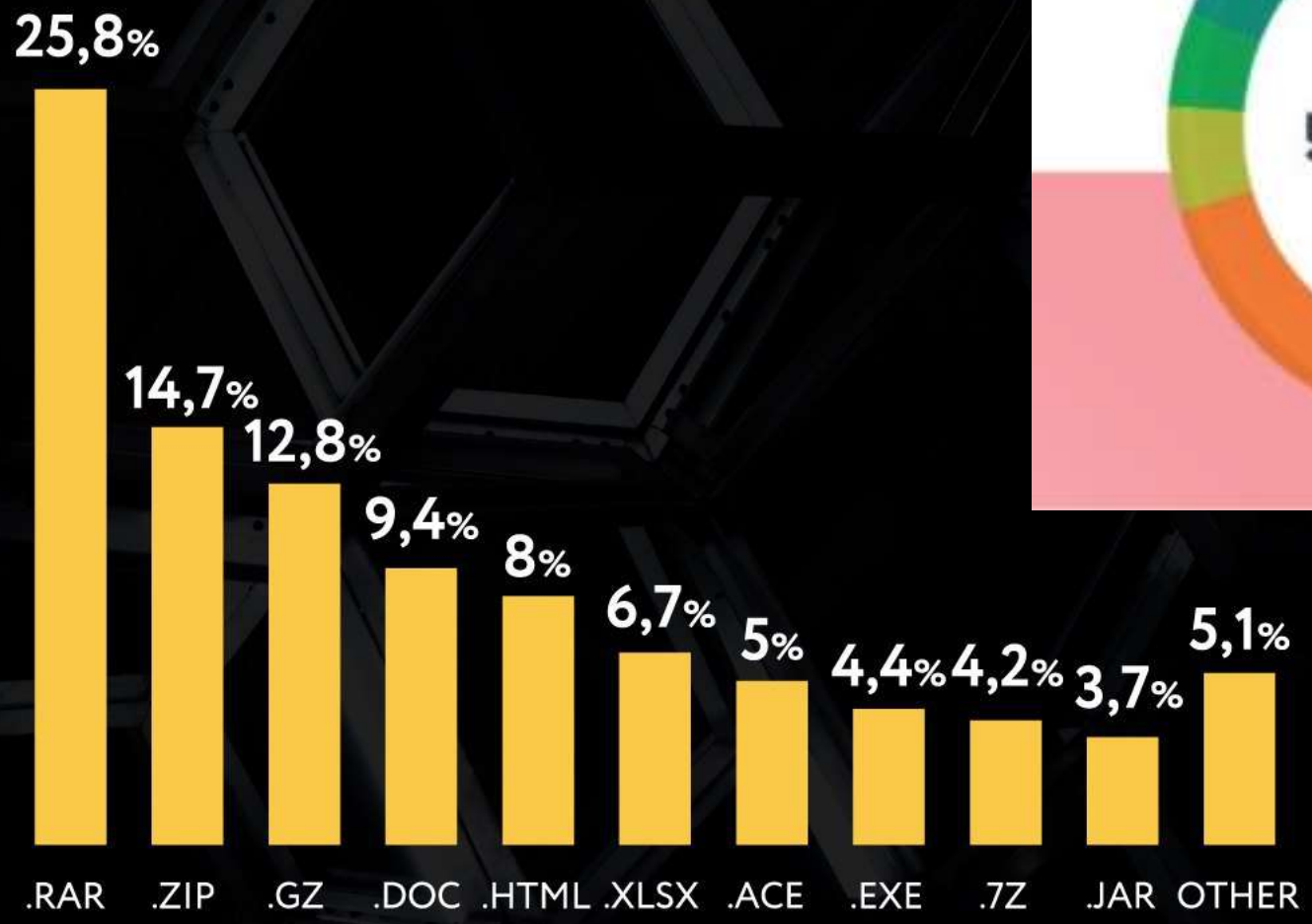
Рисунок 4. Пример фишингового письма, отправленного группой RedCurl

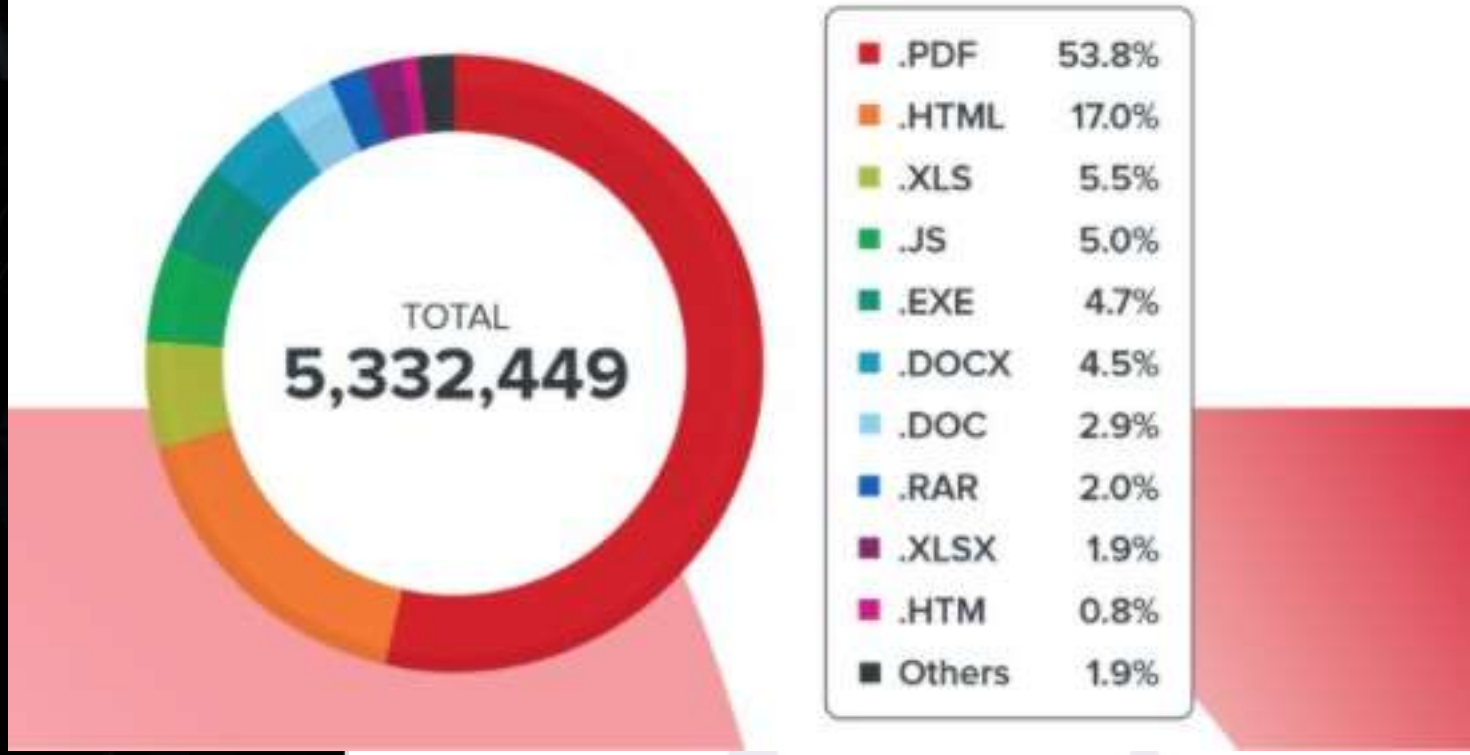
Корпоративная

Жадность

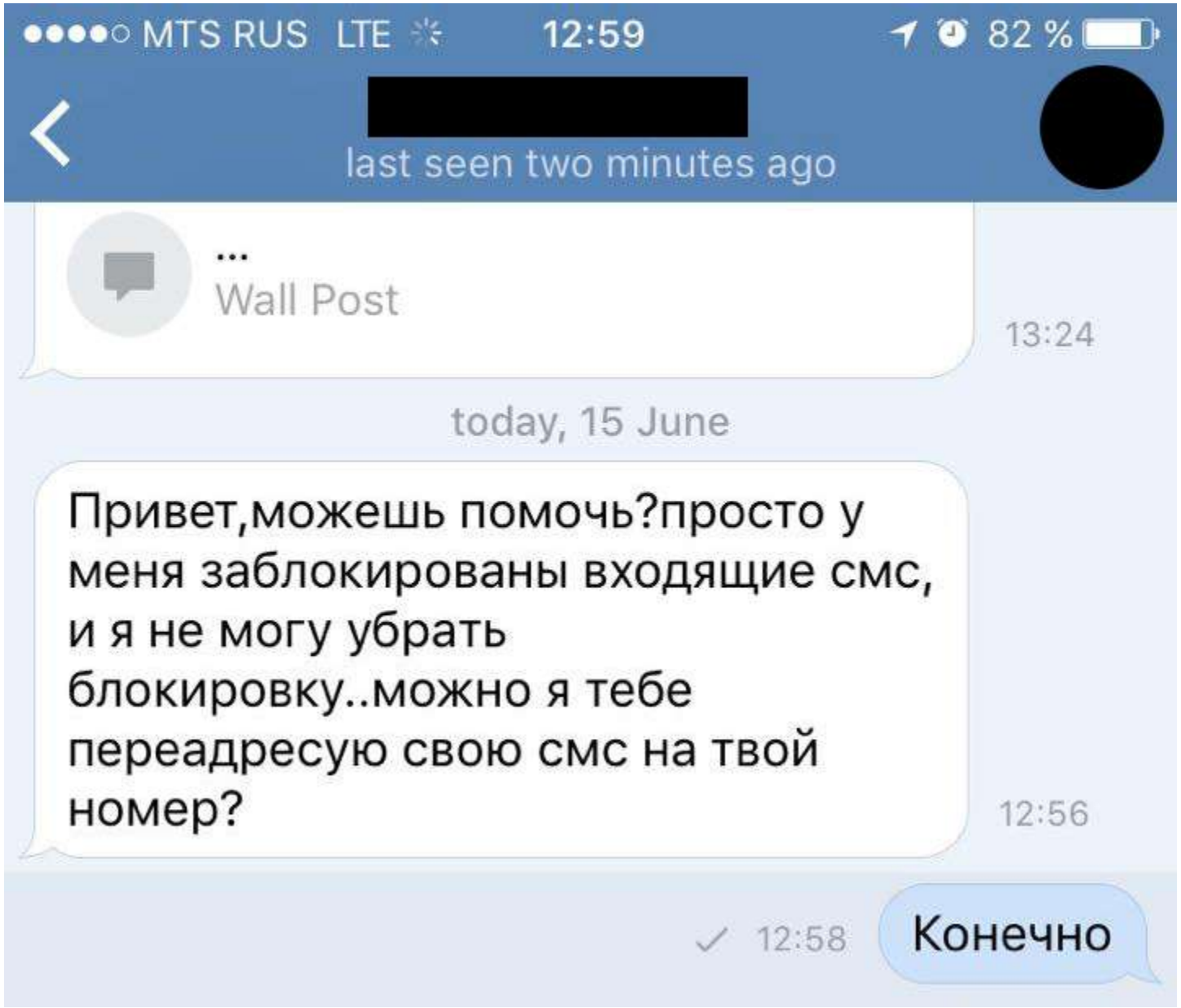
Любопытство

Расширение вредоносных вложений





Согласно данным исследования Group-IB "Депрессия шифровальщиков: топ угроз вредоносных рассылок первого полугодия 2020"



Личная

Желание помочь

Противодействие уязвимостям на 7 уровне

Обучение и тренировка навыков сотрудников


ДОБРО ПОЖАЛОВАТЬ НА КОРПОРАТИВНЫЙ ТРЕНИНГ ПО БЕЗОПАСНОСТИ.
DILBERT.COM @SCOTTADAMSSAYS
НИЧЕГО НЕ ТРОГАЙТЕ, НИКУДА НЕ ХОДИТЕ И НИ С КЕМ НЕ РАЗГОВАРИВАЙТЕ. НИКОГДА!
СПАСИБО, ЧТО ПРИШЛИ.
6-18-20 2020 Scott Adams, Inc./Dist. by Andrews McMeel
И ЭТО ВСЁ?
НЕ МОЯ ВИНА, ЧТО Я УМЕЮ КРАТКО ИЗЛАГАТЬ.

Как показывает практика, **«человеческий фактор» является ключевым и одновременно самым слабым звеном в этом процессе.**

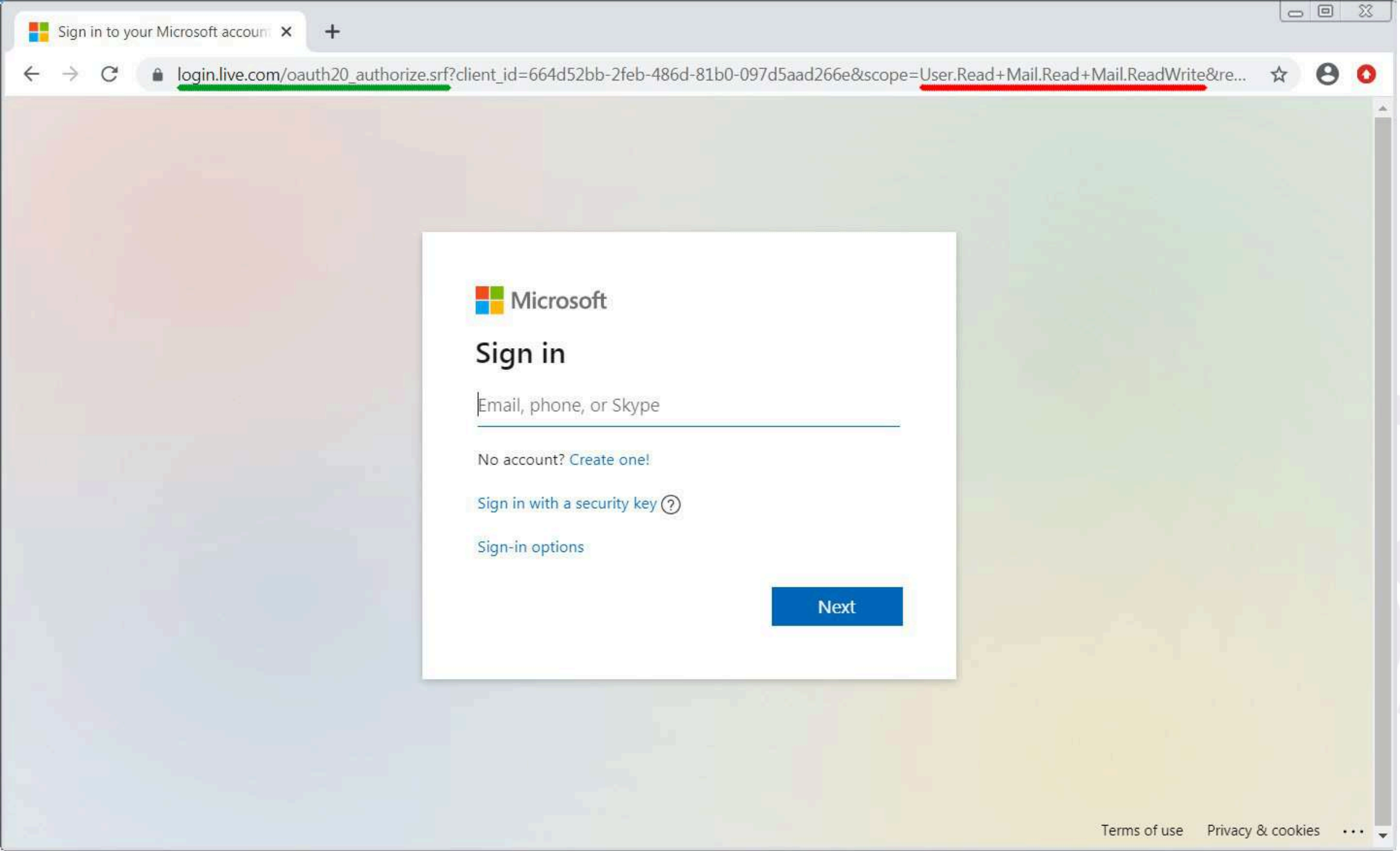
Существует ошибочное мнение, что обеспечение безопасности в информационных системах Банка - это дело исключительно специалистов в данной сфере.

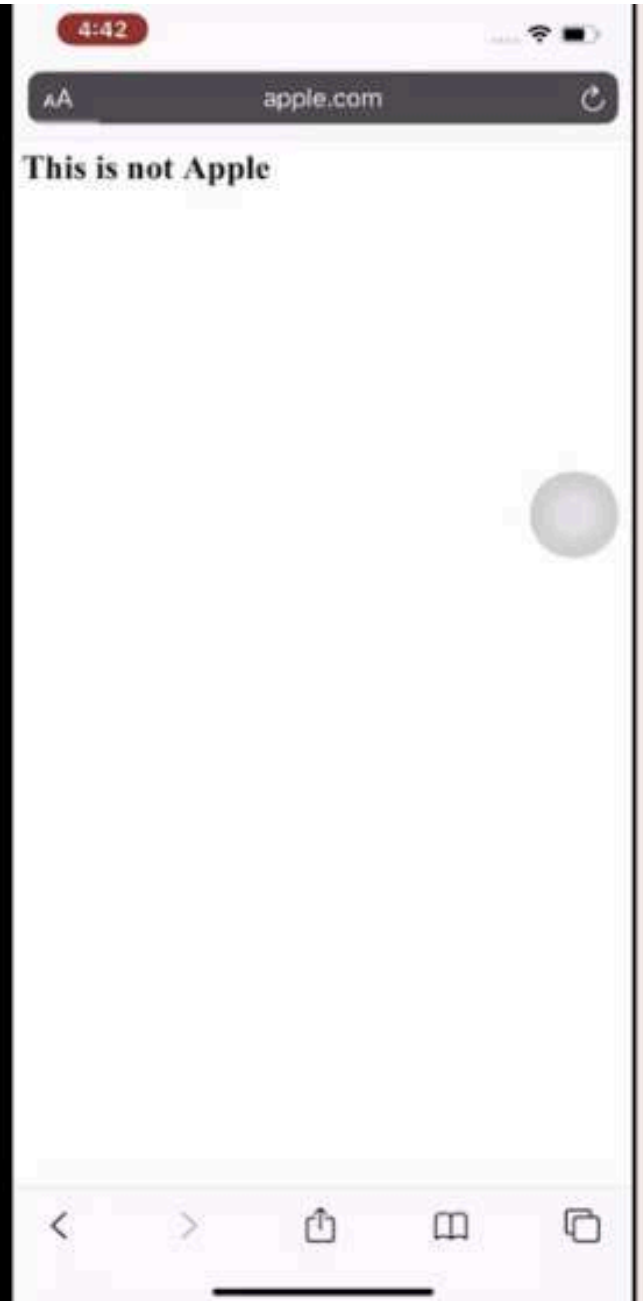
Это неверно!

Никакие технические средства защиты не помогут, если человек не будет сам осознавать серьезность данной проблемы, свое место и роль в противодействии угрозам информационной безопасности.

- Что необходимо сделать для повышения информационной безопасности?
- В чем должен выражаться вклад пользователей в общую

Искусственная среда

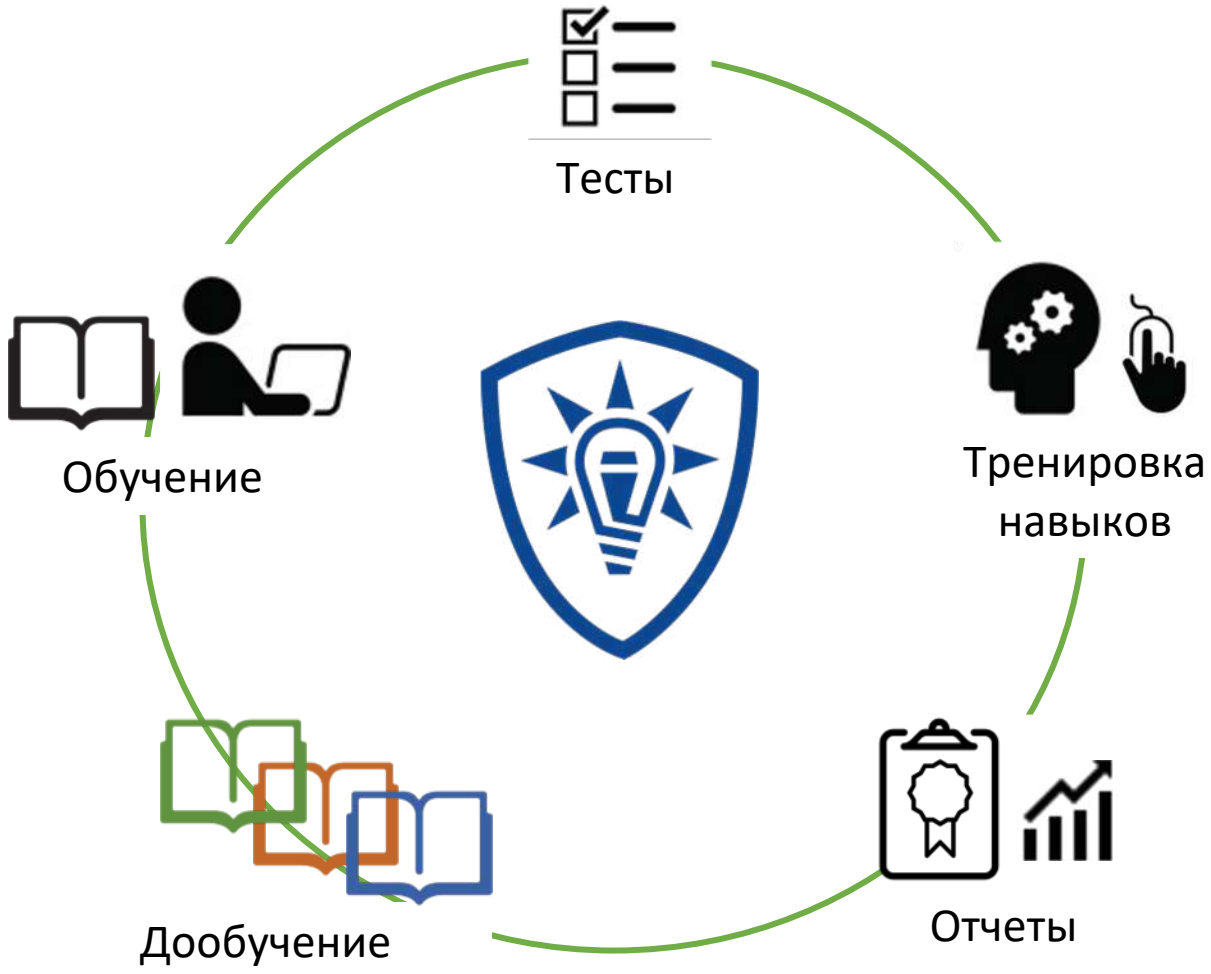

Sign in to your Microsoft accoun
login.live.com/oauth20_authorize.srf?client_id=664d52bb-2feb-486d-81b0-097d5aad266e&scope=User.Read+Mail.Read+Mail.ReadWrite&re...
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Sign in with a security key
Sign-in options
Next
Terms of use
Privacy & cookies


4:42
AA
apple.com
This is not Apple


Zong
6:51 AM
https://www.facebook.com/
This is not Facebook

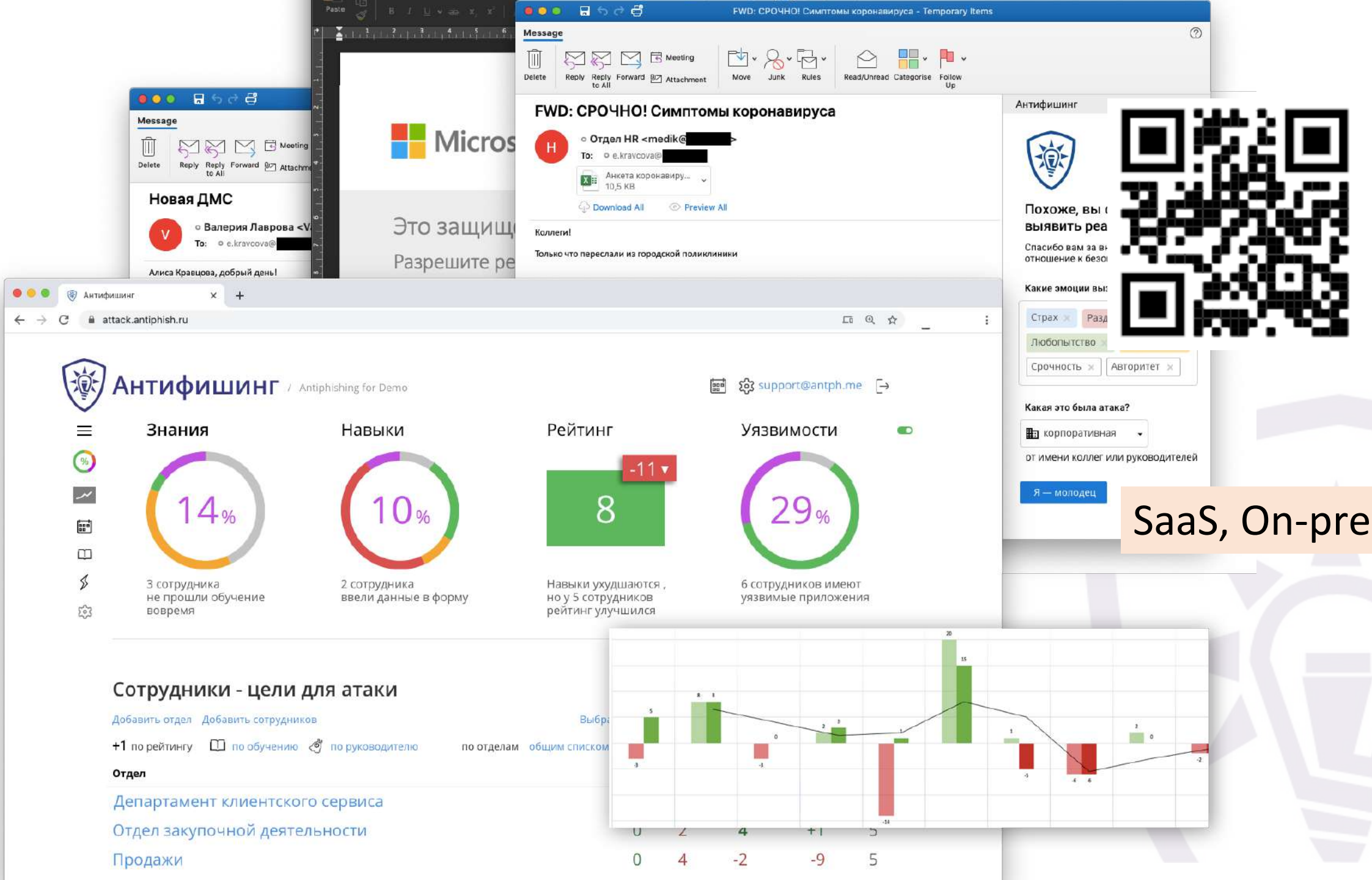

6:28
www.gmail.com:8080
This is not
Gmail.....

Антифишинг для сотрудников



Платформа для непрерывного обучения и тренировки навыков по безопасности

(Знания + Навыки) x Измерение



SaaS, On-premise

Антифишинг | Система обучени

edu.antiphish.ru/login

Антифишинг

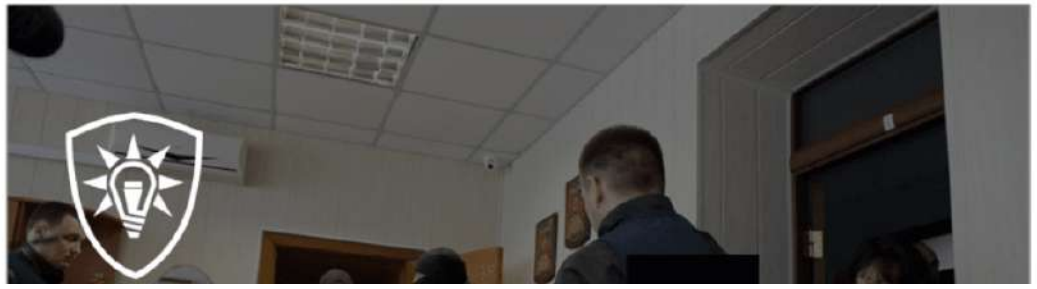
Система обучения и контроля защищенности сотрудников

Иван Алексеев
i.alekseev@antph.ru

Мои курсы Сертификаты

1. Базовый курс — до 20 ноября 2020 года

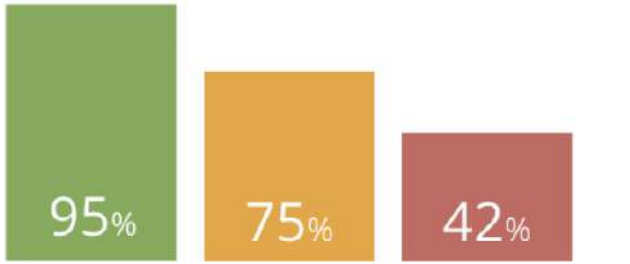
2. Основы физической безопасности — до 19 сентября 2020 года



Мой рейтинг —

Продвинутый

10 место из 141 в Департаменте клиентского сервиса
205 место из 21 200 сотрудников АО «Антифишинг»

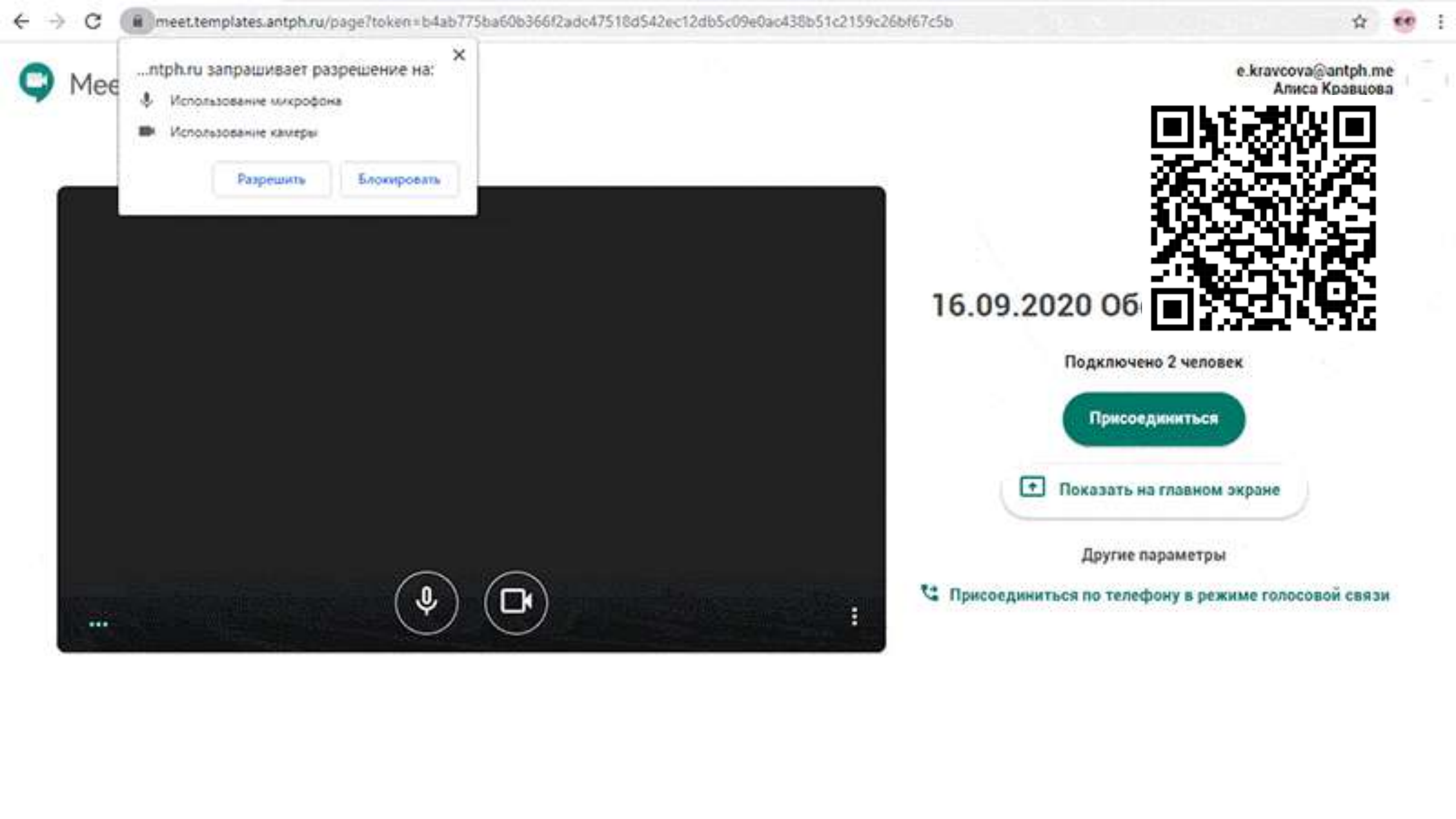


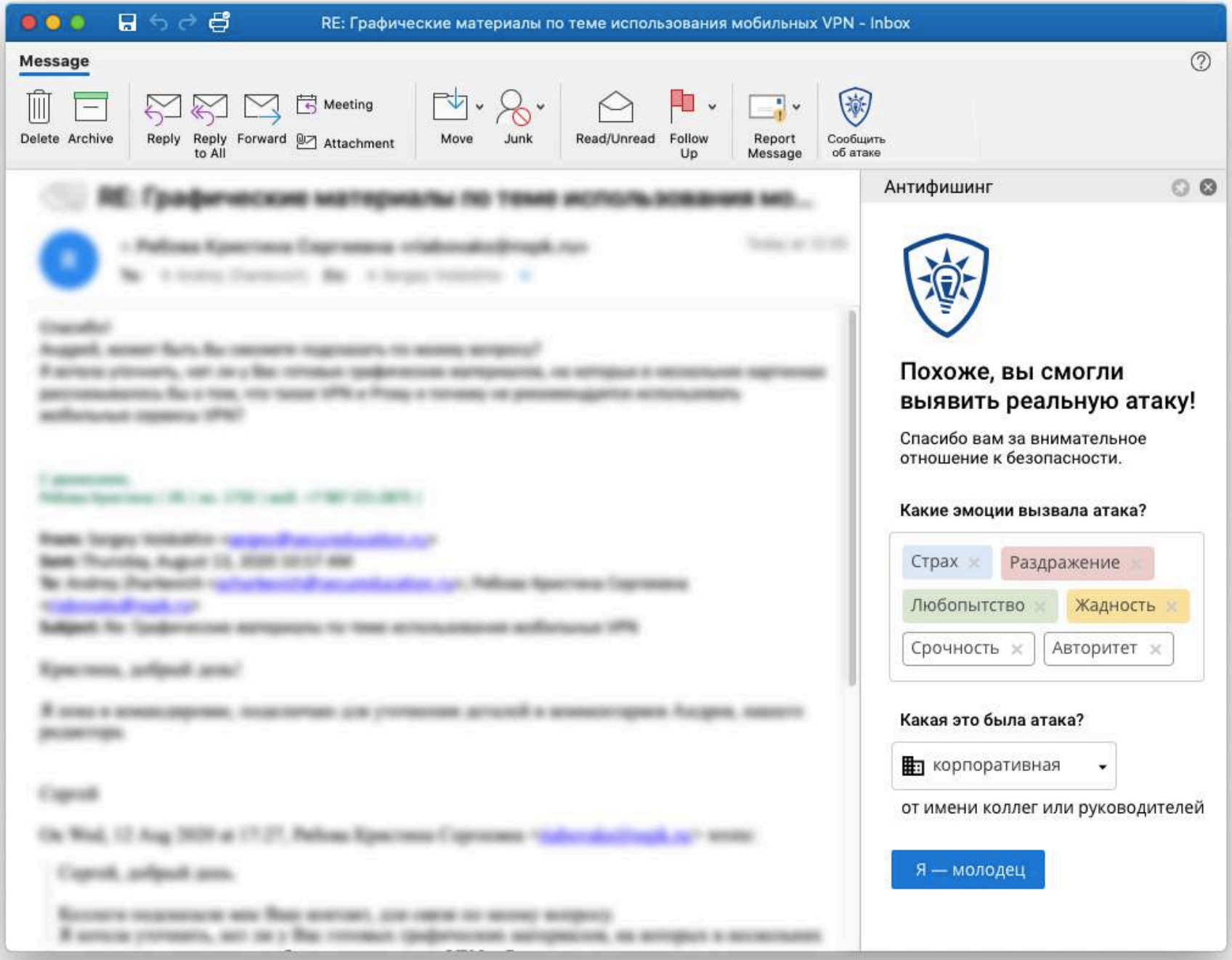
В последних трех имитированных атаках вы перешли по ссылкам, открыли вложение и ввели свой пароль на фишинговом сайте.

Самые опасные для вас эмоции

Страх × Раздражение × Жадность ×

— их пытаются вызвать мошенники в письмах, звонках и других сообщениях, чтобы вы сделали то, что им нужно.


meet.templates.antph.ru/page?token=b4ab775ba60b366f2adc47518d542ec12db5c09e0ac438b51c2159c26bf67c5b
...ntph.ru запрашивает разрешение на:
Использование микрофона
Использование камеры
Разрешить
Блокировать
e.kravcova@antph.me
Алиса Кравцова
16.09.2020 Об
Подключено 2 человек
Присоединиться
Показать на главном экране
Другие параметры
Присоединиться по телефону в режиме голосовой связи


RE: Графические материалы по теме использования мобильных VPN - Inbox
Message
Delete
Archive
Reply
Reply to All
Forward
Meeting
Attachment
Move
Junk
Read/Unread
Follow Up
Report Message
Сообщить об атаке
Антифишинг
Похоже, вы смогли выявить реальную атаку!
Спасибо вам за внимательное отношение к безопасности.
Какие эмоции вызвала атака?
Страх
Раздражение
Любопытство
Жадность
Срочность
Авторитет
Какая это была атака?
корпоративная
от имени коллег или руководителей
Я — молодец

Риски безопасности

Сохранить отчёт

Уязвимые приложения | Уязвимые сотрудники

Кол-во	Приложение и версия	Рейтинг	Комментарий
1	Macintosh Mac OS X версий 10_9_3 и ниже		Приложения содержат критические уязвимости и могут использоваться злоумышленниками для проведения атаки на пользователей, получения удаленного контроля над системой и проникновения в сеть компании. Рекомендуется обновить приложения
1	Microsoft Outlook версий 16.0.13110 и ниже		
10	Chrome версий 84.0.4147.125 и ниже		
1	Safari версий 7.0.3 и ниже		Приложения содержат незначительные уязвимости. Использование может привести к нестабильной работе или будущим рискам безопасности. Рекомендуется обновить приложения
1	Apple Mail версий 13.0 и ниже		

Дополнительные метрики по каждому сотруднику — в процессы ИБ

1. Уровень знаний

Не обучался

Прошел обучение

На обучении

Не прошел обучение вовремя

2. Уровень навыков

Выдержал атаку -5^{-2}

Сообщил об атаке

Открыл письмо 2^{-1}

Перешел по ссылке или открыл файл

Ввел данные в форму

перешел по ссылке

открыл письмо

-213 ▼

1014

3. Опасные уязвимости ПО

.NET 3.0 версий 3.0.30729 и ниже

Shockwave Flash версий 23.0 r0 и ниже

Ключевые действующие клиенты

Rostelecom

QIWI

ФИНТЕХ АССОЦИАЦИЯ

BANK SAINT PETERSBURG

GAZPROMBANK

currency·com

X5 RETAIL GROUP

белагропромбанк

Системный оператор
Единой энергетической системы

Грамотные сотрудники и клиенты – лучшая защита.

Обучайте и тренируйте своих людей.

ask@antiphish.ru

www.antiphish.ru