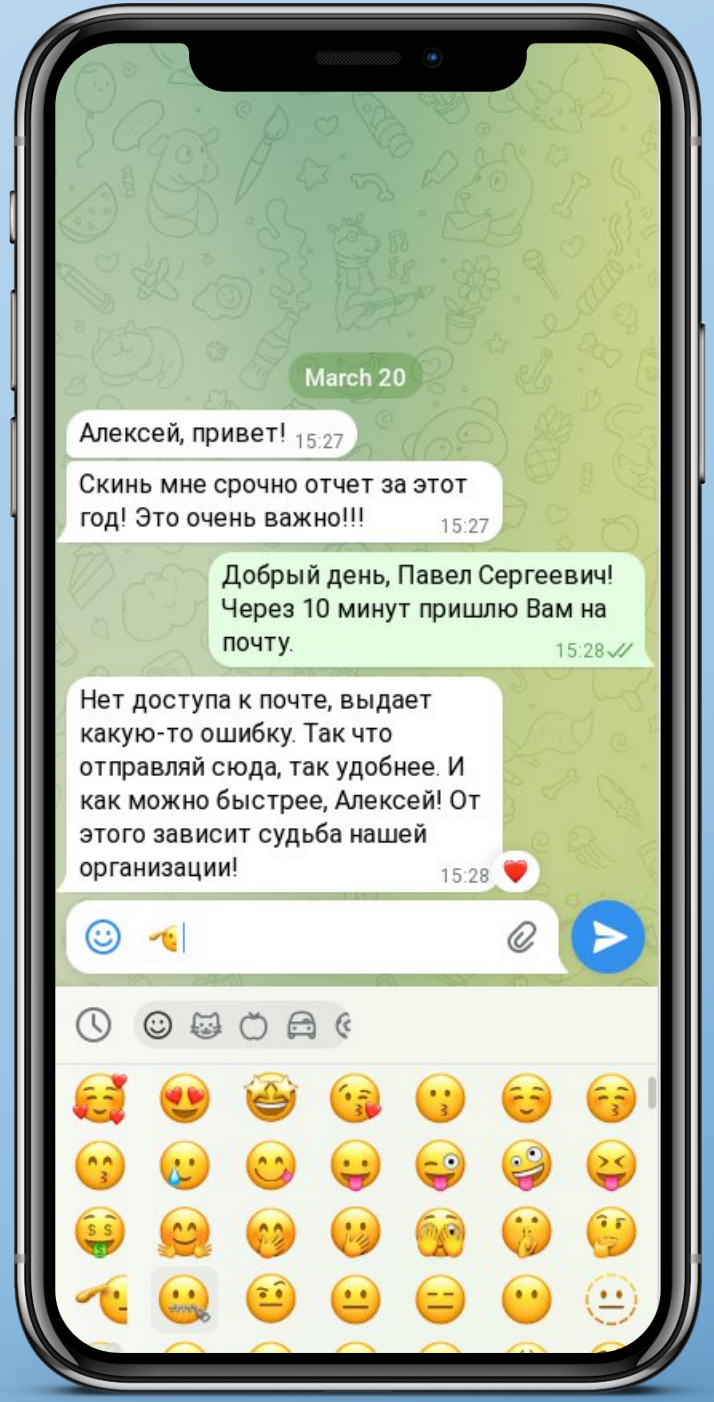
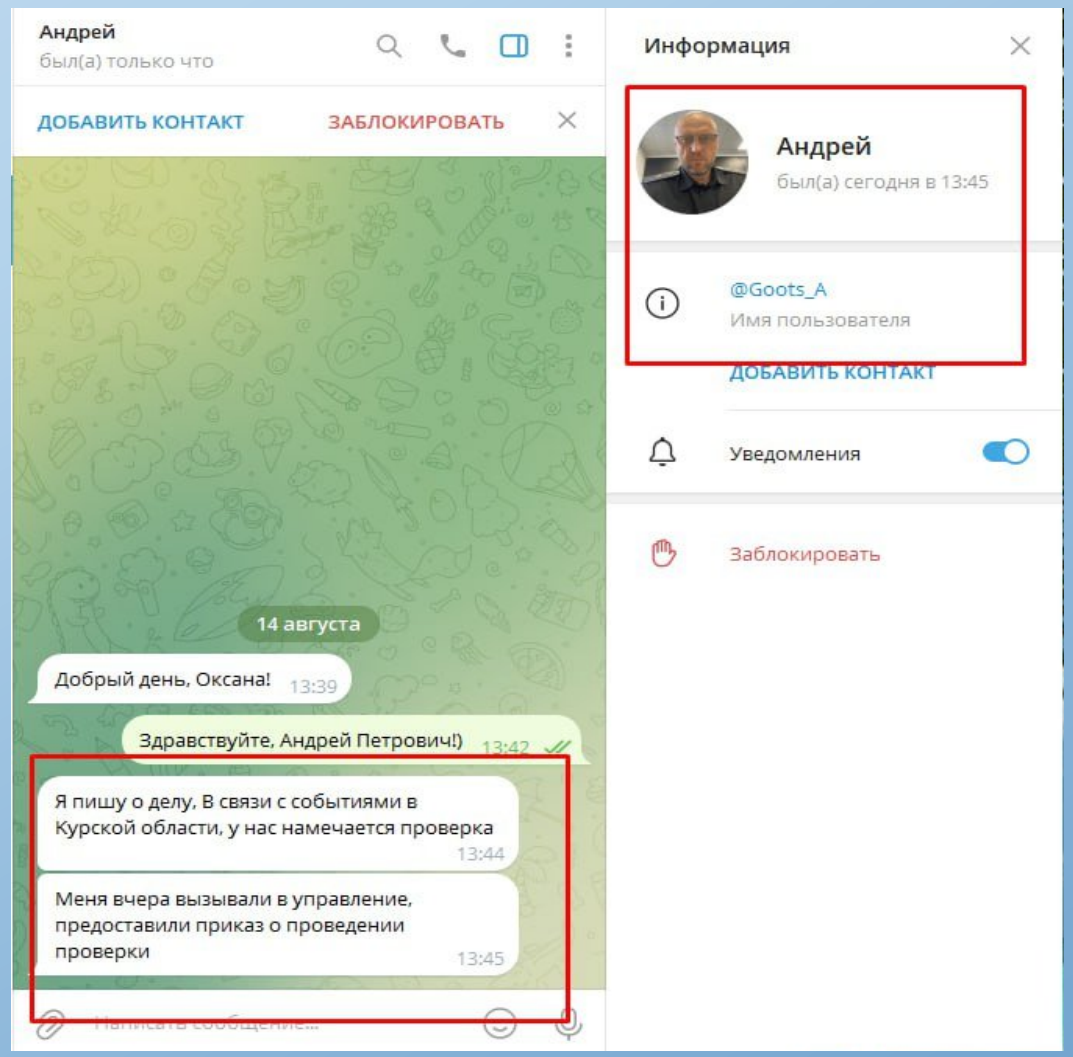


ФИШИНГ ОТ РУКОВОДИТЕЛЯ

Министерство цифрового развития Белгородской области

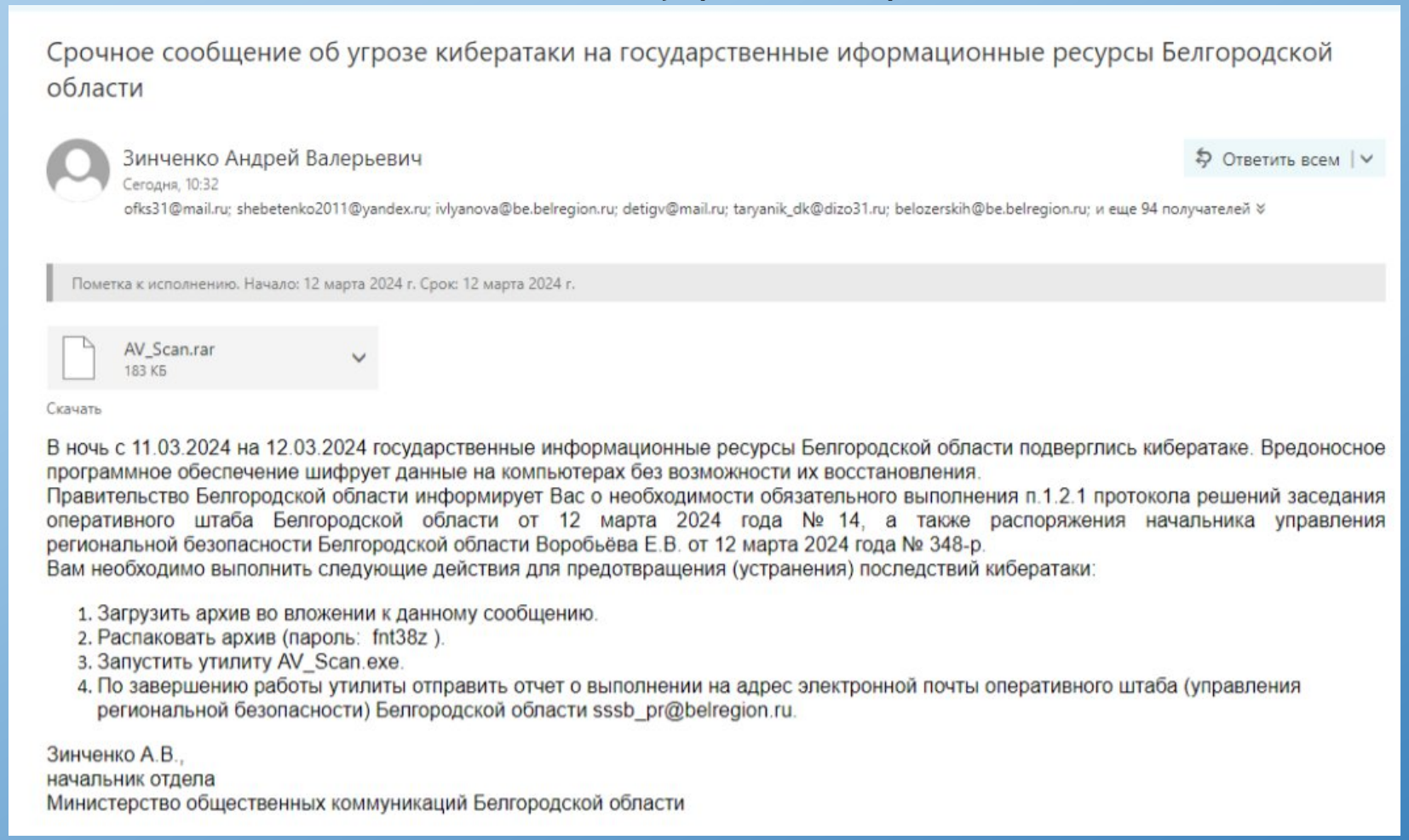
Пример фишинговых сообщений в мессенджере

Сообщения от лица якобы начальника Управления экологического и охотничьего надзора Белгородской области Гоца А.В.



Пример фишинговых сообщений на электронной почте

Сообщения с украденной учетной записи начальника отдела взаимодействия с органами власти области и муниципальными образованиями министерства общественных отношений о якобы возникшей угрозе кибератаки



Срочное сообщение об угрозе кибератаки на государственные иформационные ресурсы Белгородской области

Зинченко Андрей Валерьевич

Сегодня, 10:32

Ответить всем

ofks31@mail.ru; shebetenko2011@yandex.ru; ivlyanova@be.belregion.ru; detigv@mail.ru; taryanik_dk@dizo31.ru; belozerskih@be.belregion.ru; и еще 94 получателей

Пометка к исполнению. Начало: 12 марта 2024 г. Срок: 12 марта 2024 г.

AV_Scan.rar
183 КБ

Скачать

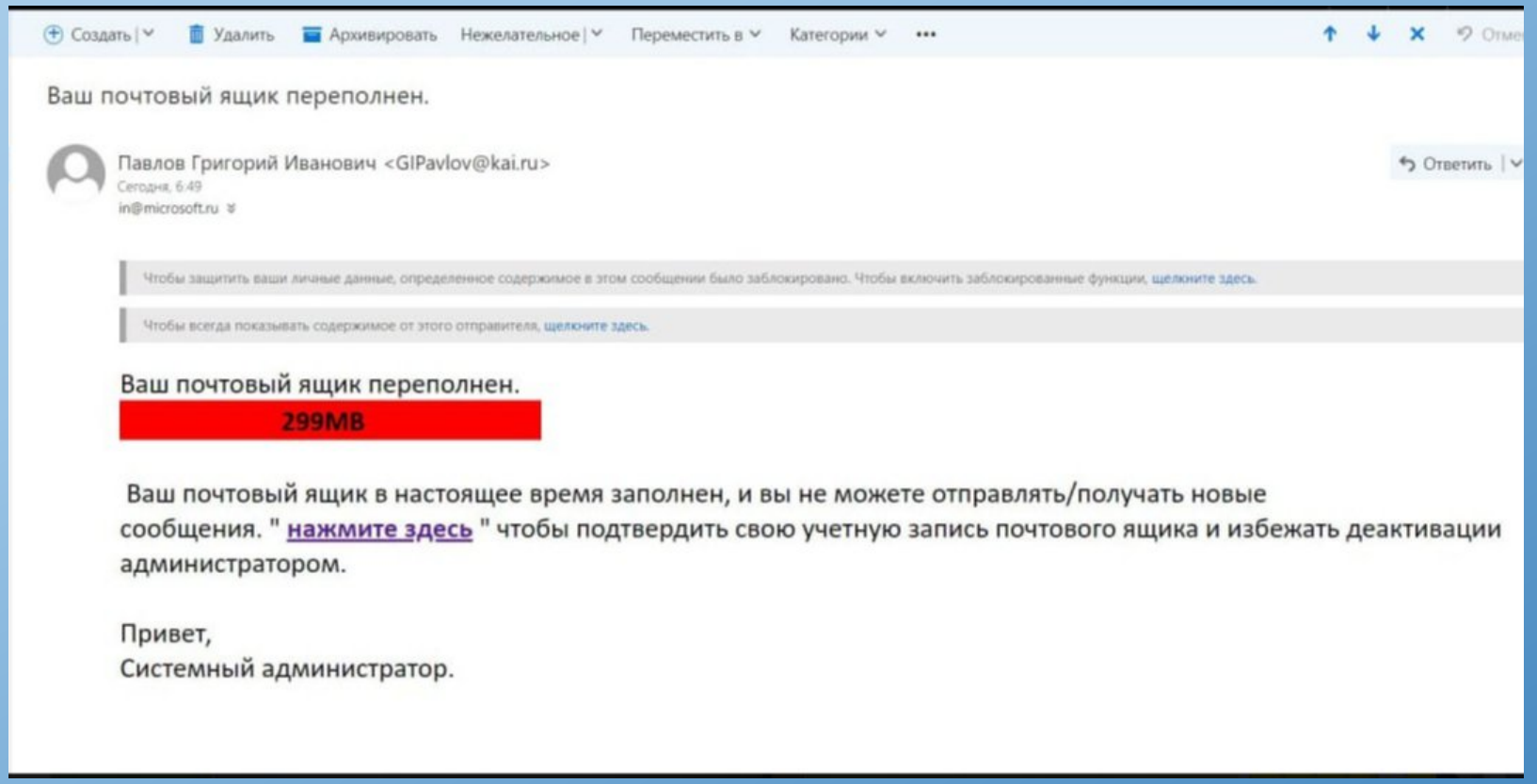
В ночь с 11.03.2024 на 12.03.2024 государственные информационные ресурсы Белгородской области подверглись кибератаке. Вредоносное программное обеспечение шифрует данные на компьютерах без возможности их восстановления.
Правительство Белгородской области информирует Вас о необходимости обязательного выполнения п.1.2.1 протокола решений заседания оперативного штаба Белгородской области от 12 марта 2024 года № 14, а также распоряжения начальника управления региональной безопасности Белгородской области Воробьёва Е.В. от 12 марта 2024 года № 348-р.
Вам необходимо выполнить следующие действия для предотвращения (устранения) последствий кибератаки:

1. Загрузить архив во вложении к данному сообщению.
2. Распаковать архив (пароль: fnt38z).
3. Запустить утилиту AV_Scan.exe.
4. По завершению работы утилиты отправить отчет о выполнении на адрес электронной почты оперативного штаба (управления региональной безопасности) Белгородской области sssb_pr@belregion.ru.

Зинченко А.В.,
начальник отдела
Министерство общественных коммуникаций Белгородской области

Пример фишинговых сообщений на электронной почте

Сообщения о переполненном почтовом ящике от якобы системного администратора организации

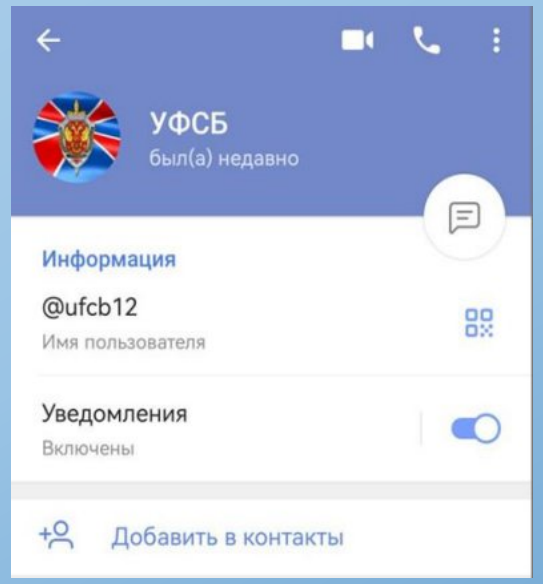


Уловки мошенников. Примеры

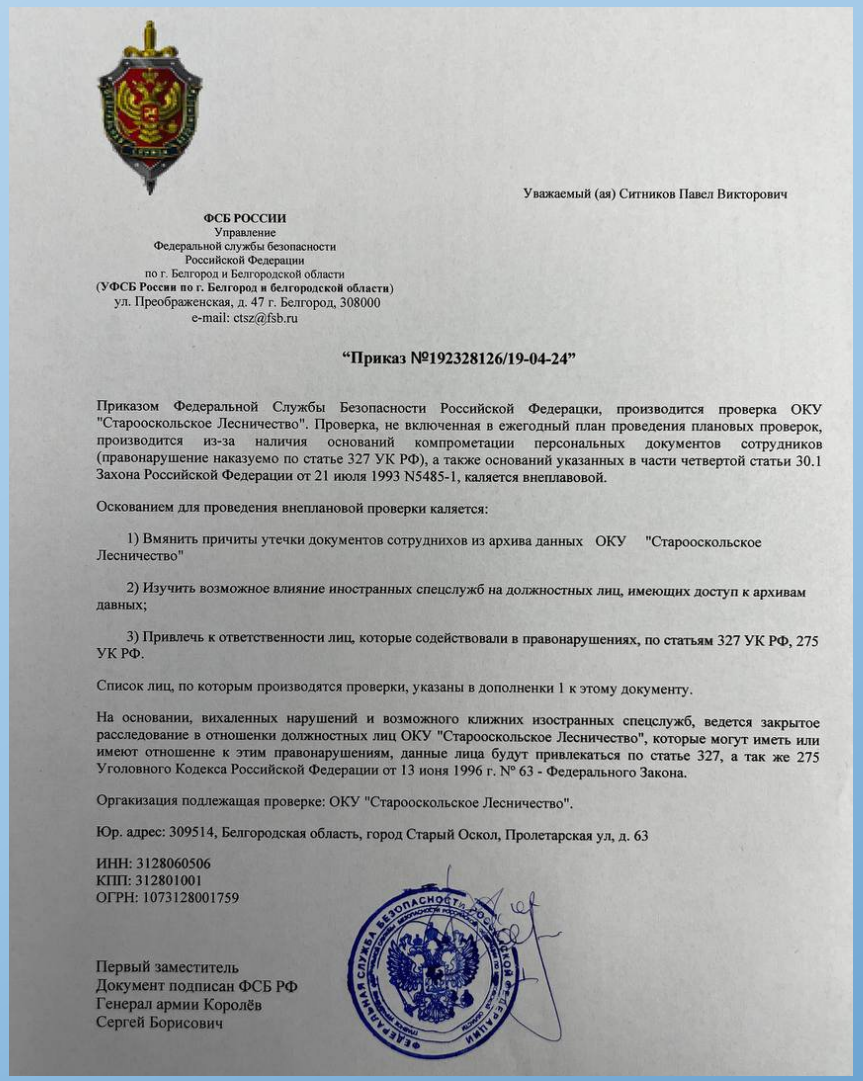
Подменяют номер телефона на официальный

Направляют фото якобы своего служебного удостоверения

Используют официальную символику органов государственных власти



Уловки мошенников. Примеры



Уважаемый (ая) Ситников Павел Викторович

ФСБ РОССИИ
Управление
Федеральной службы безопасности
Российской Федерации
по г. Белгород и Белгородской области
(УФСБ России по г. Белгород и белгородской области)
ул. Преображенская, д. 47 г. Белгород, 308000
e-mail: ctsz@fsb.ru

“Приказ №192328126/19-04-24”

Приказом Федеральной Службы Безопасности Российской Федерацки, производится проверка ОКУ "Старооскольское Лесничество". Проверка, не включенная в ежегодный план проведения плановых проверок, производится из-за наличия оснований компрометации персональных документов сотрудников (правонарушение наказуемо по статье 327 УК РФ), а также оснований указанных в части четвертой статьи 30.1 Захона Российской Федерации от 21 июля 1993 N5485-1, каляется внеплавовой.

Оскованием для проведения внеплановой проверки каляется:

1) Вмянить причиты утечки документов сотруднихов из архива данных ОКУ "Старооскольское Лесничество"

2) Изучить возможное влияние иностранных спецслужб на должностных лиц, имеющих доступ к архивам давных;

3) Привлечь к ответственности лиц, которые содействовали в правонарушениях, по статьям 327 УК РФ, 275 УК РФ.

Список лиц, по которым производятся проверки, указаны в дополненки 1 к этому документу.

На основании, вихаленных нарушений и возможного клижних изостранных спецслужб, ведется закрытое расследование в отношенки должностных лиц ОКУ "Старооскольское Лесничество", которые могут иметь или имеют отношенне к этим правонарушениям, данные лица будут привлекаться по статье 327, а так же 275 Уголовного Кодекса Российской Федерации от 13 ионя 1996 г. № 63 - Федерального Закона.

Оргакизация подлежащая проверке: ОКУ "Старооскольское Лесничество".

Юр. адрес: 309514, Белгородская область, город Старый Оскол, Пролетарская ул, д. 63

ИНН: 3128060506
КПП: 312801001
ОГРН: 1073128001759

Первый заместитель
Документ подписан ФСБ РФ
Генерал армии Королёв
Сергей Борисович

Мошенники направляют от имени органа государственной власти (УФСБ России по Белгородской области) якобы официальное обращение, заверенное подписью и печатью руководителя, о проведении внеплановой проверки органа (организации) и привлечении к ответственности сотрудников

Уловки мошенников. Примеры

Банк России ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: d107312a3a9a80b8543c329adbbf9abb
Владелец: А. С. Набережный
Действителен с 07.10.2022 по 06.03.2024

Банк России
Центральный банк Российской Федерации

Исх. № 53517742 г. Москва

Документ № 53517742

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы, , стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого лицевого счета.
Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Переоформление кредитной заявки.
Если в системе банков отображается активная заявка на кредит - её необходимо отклонить, путем подачи новой заявки. Финансы для проведения операции по отклонению кредитной заявки предоставляются из резервного фонда ЦБ РФ (согласно ФЗ "О противодействии отмывания доходов, полученных преступным путем, и финансированию терроризма", в целях совершенствования контроля). Данная заявка не будет отображаться в кредитной истории и не влияет на кредитный рейтинг в дальнейшем.

II этап:
- Погашение кредитнорй задолженности.
Выполняется методом внесения финансовых активов, предоставленных вам из резервных фондов ЦБ РФ. Внесение выполняется зашифрованным методом (с помощью АТМ устройства, рассчетно-кассового центра страхового банка партнера), предоставленным отделом финансового мониторинга.

III этап:
После выполнения всех регламентных работ, представителем ЦБ РФ будет назначено время и адрес отделения банка в которое клиенту необходимо явиться для: актуализации паспортных данных, перевыпуска пластиковых носителей, подписания и получения документации.

Уведомляем Вас
- о наступлении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (Согласно ст. 183 УК РФ (соблюдение политики конфиденциальности, коммерческой, налоговой и банковской тайны)).
- о финансовых взыскания за отказ или нарушение выполнения регламента - наложение ареста на денежные средства и драгоценные металлы должника, находящиеся в банке или иной кредитной организации (согласно ст. 81 УК РФ) и взыскании денежных средств, выделенных Банком для выполнения регламентных действий (выпуск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

Срок обновления реквизитов с момента выполненных работ, составляет 2 часа.
Специалист Банка России: Беляев Роман Алексеевич.
Финансово-ответственное лицо: Ожидает закрытие кредитного договора.

Зам. Начальника ОДИО РОО "Москва" филиала №3 ЦБ РФ
М.П.

А. С. Набережный

Мошенники направляют от имени органа государственной власти (Банк России) якобы официальное обращение, заверенное подписью и печатью руководителя, о необходимости выполнения процедуры обновления единого лицевого счета

Что делать, если вы получили письмо от лица руководителя вашей организации?

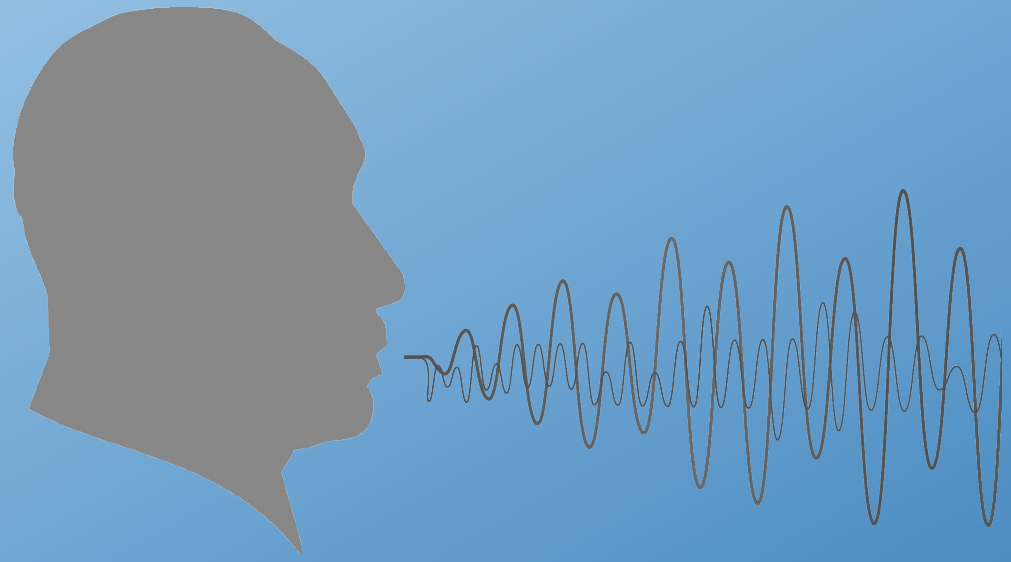
- ✓ **Прекратите какое-либо общение с мошенником.** Вас могут начать пугать фотографиями служебных удостоверений, официальных документов и тому подобным. **Не поддавайтесь давлению!**
- ✓ **Расскажите своему непосредственному руководителю** о факте обращения от лица руководителя Департамента или вашей организации
- ✓ **Дождитесь** от непосредственного руководителя **подтверждения достоверности обращения** от руководителя Департамента или организации
- ✓ В случае, если это всё-таки были мошенники, **напишите об инциденте на почту:** ddd@belregion.ru и avz@belregion.ru
- ✓ В случаях, если вы подверглись манипуляции и совершили какие-либо действия со своим банковским счетом, **немедленно обращайтесь в банк** для блокирования переводов и **в правоохранительные органы** – с заявлением о мошенничестве

«От имени руководителя» - теперь и голосом

Используя современные технологии, мошенники генерируют фейковые **ГОЛОСОВЫЕ СООБЩЕНИЯ**, которые отправляют через **мессенджеры**

Будьте бдительны если:

- сообщение выходит за рамки привычного обсуждения – например, связано с денежным переводом, запросом пароля, необходимостью взаимодействия с правоохранительными органами и т.п.
- вы не ждали личного сообщения от руководителя
- в сообщении присутствует давление через свой авторитет
- в сообщении присутствует момент срочности



ФСТЭК России рекомендует

Письма ФСТЭК России

От 29.12.2023 № 240/22/6370

«…Хакерской группировкой Core Werewolf осуществляются компьютерные атаки на информационную инфраструктуру РФ, путем направления от имени ФСТЭК России «фишинговых» электронных писем с именем домена отправителя «cfo_11otd@fstec.support.», содержащих вредоносный архив с наименованием «Меры. Список уязвимостей и принимаемых мер по их устранению.exe»...»

От 19.01.2024 № 240/91/208

«…Хакерской APT-группировкой Sticky Werewolf в адрес ФОИВ, субъектов КИИ и организаций РФ направляются фишинговые письма от имени ФСБ России, МЧС России и Минстроя России, а также иных органов и организаций, содержащие вредоносные вложения (трояны Darktrack RAT, Ozone RAT, стилер MetaStealer)»...».

Обращаем внимание!

- ✓ ФСТЭК России осуществляет взаимодействие посредством системы МЭДО, почтовой связи и электронной почты (домен @fstec.ru).
- ✓ При получении электронного письма от имени ФСТЭК России, необходимо связаться с ответственным исполнителем по ранее направленным ФСТЭК России письмам, перезвонив ему по телефону

Всегда на связи!

Министерство
цифрового развития
Белгородской
области

ddd@belregion.ru