ПРОТИВОДЕЙСТВИЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ПЕРСОНАЛОМ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ

Комаров Валерий Валерьевич

Департамент
информационных
технологий
города Москвы

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

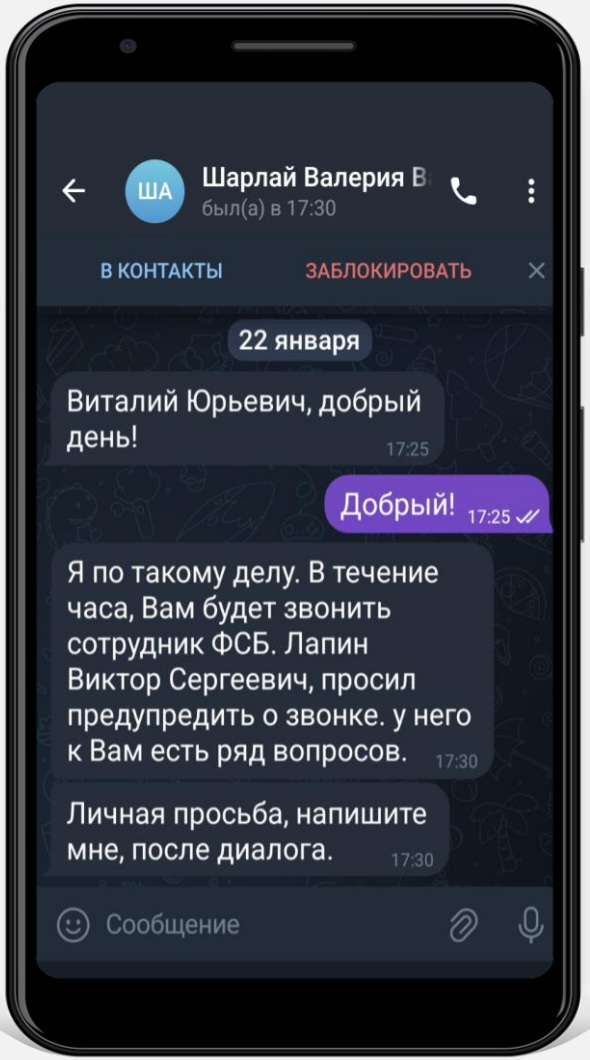
Метод управления действиями человека без использования технических средств, заключающийся в **использовании слабостей человеческого фактора**

Цель:

- *незаконное получение конфиденциальной информации, паролей, банковских данных, доступа к устройству жертвы.*

- ФИШИНГ В МЕССЕНДЖЕРАХ

ПРИМЕР ФИШИНГОВЫХ СООБЩЕНИЙ ОТ ЛИЦА РУКОВОДИТЕЛЯ ОРГАНИЗАЦИИ

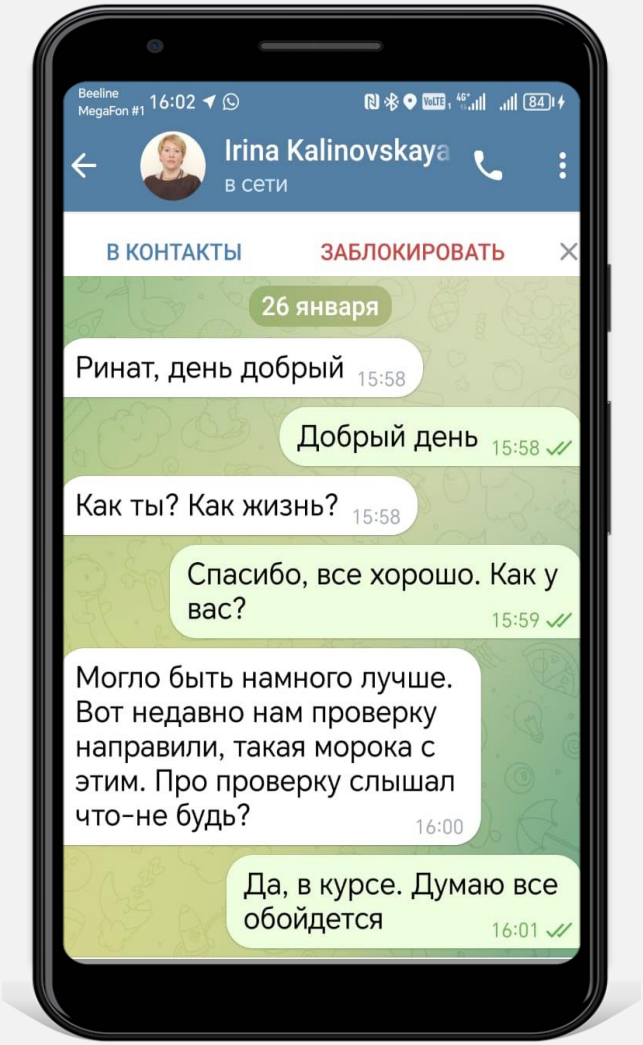


Получение сообщение от лица руководителя организации
(мошенник использует официальное фото на аватарке, реальные фамилию, имя и отчество)

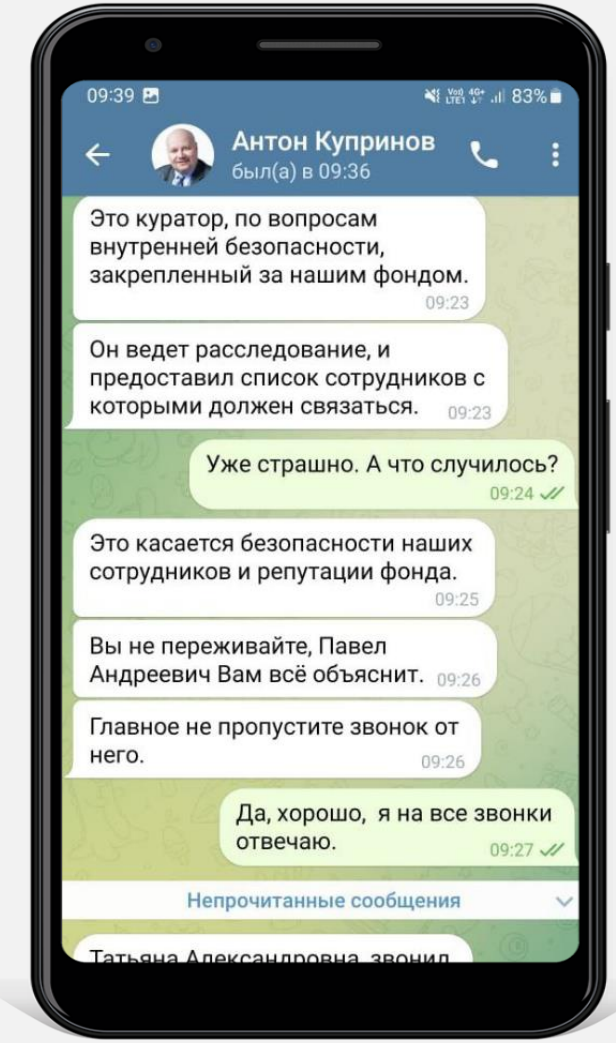
Используется **давление на человека через авторитет и репутацию** руководителя, подготовка к общению с лже-сотрудником ФСБ

Продолжение переписки может привести к **финансовым потерям, хищению личной и конфиденциальной информации и подрыву репутации**

ЕЩЕ ПРИМЕРЫ


Beeline
MegaFon #1
16:02
Irina Kalinovskaya
в сети
В КОНТАКТЫ
ЗАБЛОКИРОВАТЬ
26 января
Ринат, день добрый 15:58
Добрый день 15:58
Как ты? Как жизнь? 15:58
Спасибо, все хорошо. Как у вас? 15:59
Могло быть намного лучше. Вот недавно нам проверку направили, такая морока с этим. Про проверку слышал что-не будь? 16:00
Да, в курсе. Думаю все обойдется 16:01


WhatsApp
14:34
100 %
Назад
Alexey Emelyanov
печатает
Заблокировать
Добавить
Сегодня
Аня, добрый день 14:29
Добрый день! 14:32
Как ты? Как жизнь? 14:33
Нормально! 14:33
Ну вот и хорошо. Я вообще по делу пишу. К нам проверка была направлена, слышала про это? 14:34
Нет 14:34
Сообщение

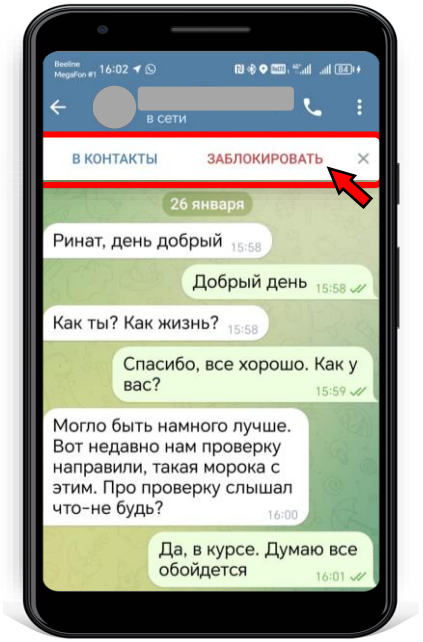

09:39
83%
Антон Купринов
был(а) в 09:36
Это куратор, по вопросам внутренней безопасности, закрепленный за нашим фондом. 09:23
Он ведет расследование, и предоставил список сотрудников с которыми должен связаться. 09:23
Уже страшно. А что случилось? 09:24
Это касается безопасности наших сотрудников и репутации фонда. 09:25
Вы не переживайте, Павел Андреевич Вам всё объяснит. 09:26
Главное не пропустите звонок от него. 09:26
Да, хорошо, я на все звонки отвечаю. 09:27
Непрочитанные сообщения

ПРОВЕРКА ПРОФИЛЯ ПРИ ПОЛУЧЕНИИ СООБЩЕНИЯ ОТ РУКОВОДИТЕЛЯ

ДИТ

1 Просмотр профиля

- Обратите внимание на оповещение смартфона об отсутствии контакта в телефонной книге.



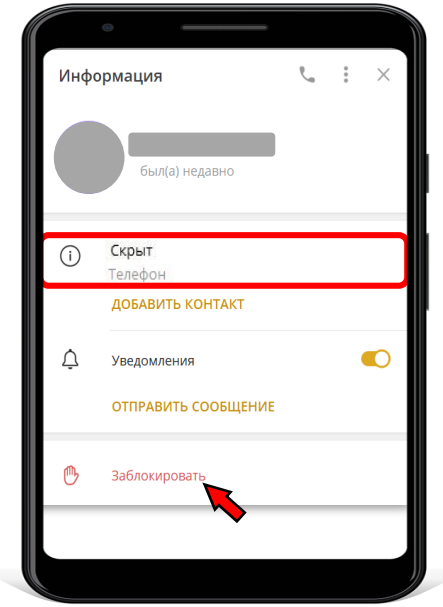
Если контакта нет в телефонной книге, то появятся кнопки «Заблокировать» и «В контакты»

2 Незнакомый номер

- Перезвоните в приемную руководителя по телефону из справочника Правительства Москвы.
- Не используйте телефонный номер обратившегося абонента.
- При отсутствии подтверждения от приемной выберите пункт меню «Заблокировать».

3 Важно!

- Если номер скрыт в профиле, то блокируйте обратившегося и не поддерживайте общение с ним.

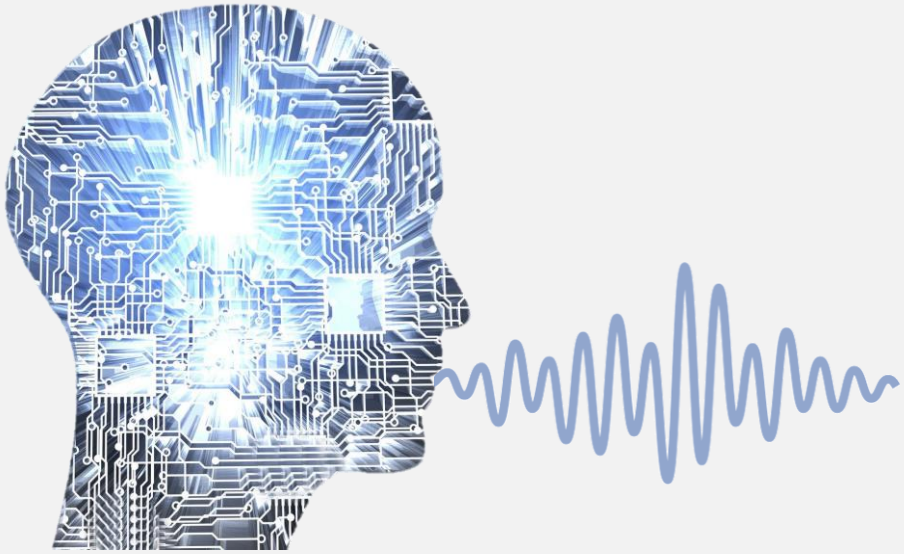


«ОТ ИМЕНИ РУКОВОДИТЕЛЯ» - ТЕПЕРЬ ГОЛОСОМ

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**



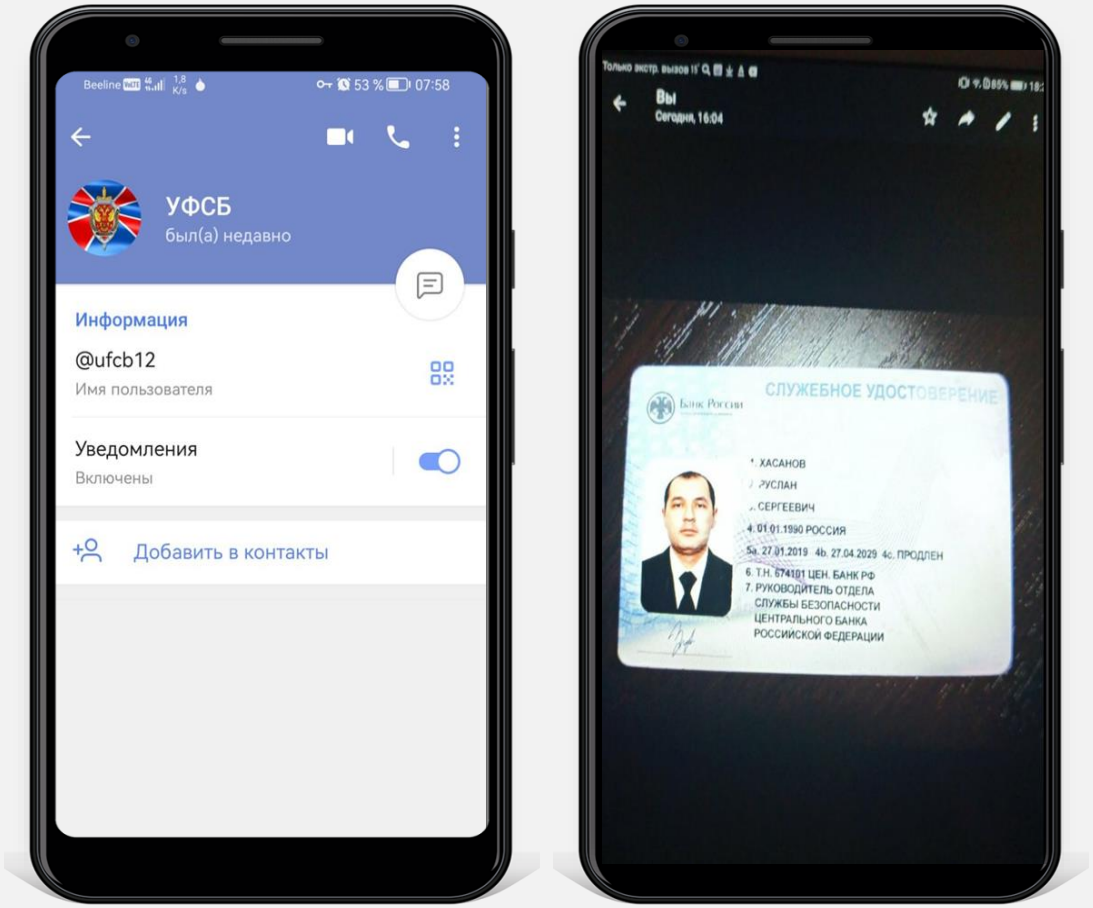
КАК ПОСТУПИТЬ ПРИ ПОЛУЧЕНИИ СООБЩЕНИЯ ОТ ЛИЦА РУКОВОДИТЕЛЯ?

ДИТ

- ✓ **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 этом на почту:** DITantifishing@mos.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**

ПРИМЕРЫ УЛОВОК МОШЕННИКОВ

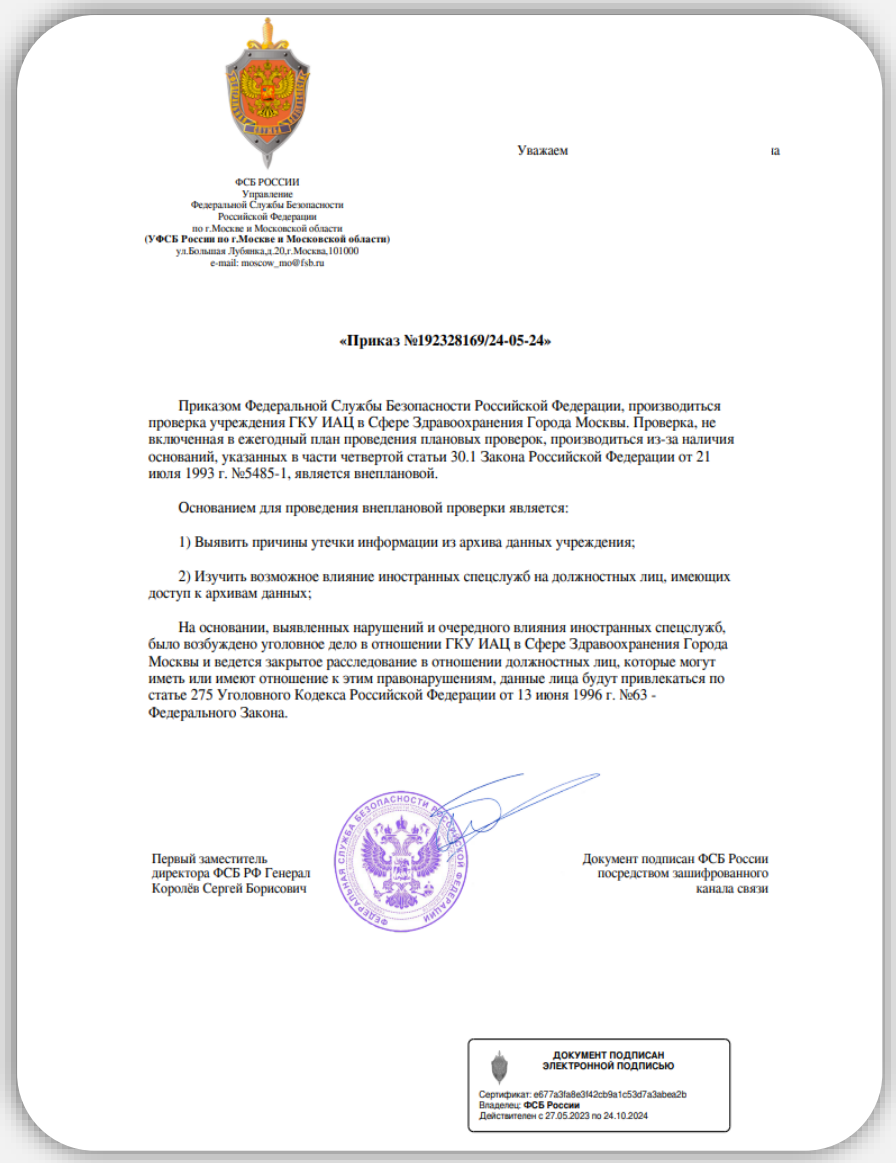
- Подменяют номер телефона на официальный
- Направляют фото якобы своего служебного удостоверения
- Используют официальную символику органов государственных власти



ПРИМЕРЫ УЛОВОК МОШЕННИКОВ

Мошенники направляют сообщение в мессенджере от имени органа государственной власти в виде вложения письма:

- На рисунке якобы **приказ УФСБ России по Московской области о проведении внеплановой проверки**, заверенный подписью и печатью руководителя, о голосовом согласии в сотрудничестве с органами государственной власти



ФСБ РОССИИ
Управление
Федеральной Службы Безопасности
Российской Федерации
по г.Москве и Московской области
(УФСБ России по г.Москве и Московской области)
ул.Большая Лубянка,д.20,г.Москва,101000
e-mail: moscow_mo@fsb.ru

Уважаем ца

«Приказ №192328169/24-05-24»

Приказом Федеральной Службы Безопасности Российской Федерации, производиться проверка учреждения ГКУ ИАЦ в Сфере Здравоохранения Города Москвы. Проверка, не включенная в ежегодный план проведения плановых проверок, производиться из-за наличия оснований, указанных в части четвертой статьи 30.1 Закона Российской Федерации от 21 июля 1993 г. №5485-1, является внеплановой.

Основанием для проведения внеплановой проверки является:

1) Выявить причины утечки информации из архива данных учреждения;

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

На основании, выявленных нарушений и очередного влияния иностранных спецслужб, было возбуждено уголовное дело в отношении ГКУ ИАЦ в Сфере Здравоохранения Города Москвы и ведется закрытое расследование в отношении должностных лиц, которые могут иметь или имеют отношение к этим правонарушениям, данные лица будут привлекаться по статье 275 Уголовного Кодекса Российской Федерации от 13 июня 1996 г. №63 - Федерального Закона.

Первый заместитель
директора ФСБ РФ Генерал
Королёв Сергей Борисович

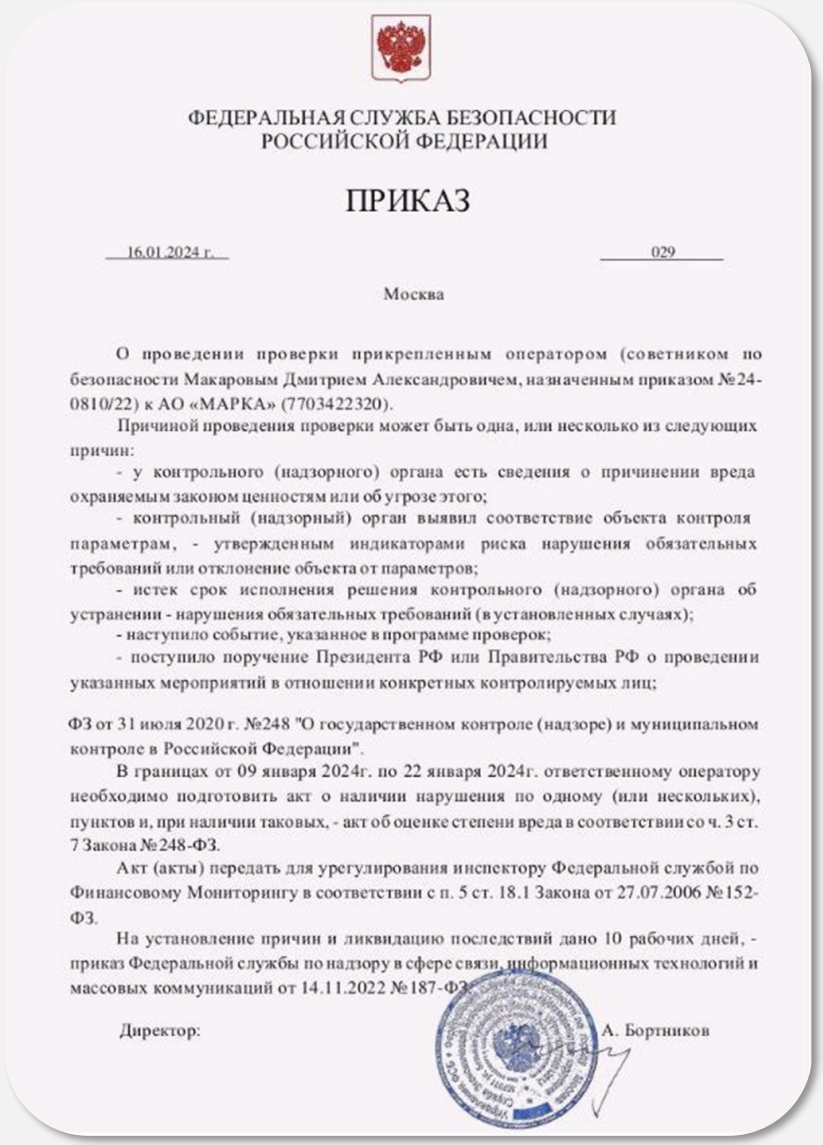
Документ подписан ФСБ России
посредством зашифрованного
канала связи

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: e677a3fa8e3f42cb9a1c53d7a3abea2b
Владелец: **ФСБ России**
Действителен с 27.05.2023 по 24.10.2024

ПРИМЕРЫ УЛОВОК МОШЕННИКОВ

Мошенники направляют сообщение в мессенджере от имени органа государственной власти в виде вложения письма:

- На рисунке **приказ ФСБ России** о **проведении проверки прикрепленным оператором**, заверенный подписью и печатью руководителя, о голосовом согласии в сотрудничестве с органами государственной власти



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

16.01.2024 г. 029

Москва

О проведении проверки прикрепленным оператором (советником по безопасности Макаровым Дмитрием Александровичем, назначенным приказом №24-0810/22) к АО «МАРКА» (7703422320).

Причиной проведения проверки может быть одна, или несколько из следующих причин:

- у контрольного (надзорного) органа есть сведения о причинении вреда охраняемым законом ценностям или об угрозе этого;
- контрольный (надзорный) орган выявил соответствие объекта контроля параметрам, - утвержденным индикаторами риска нарушения обязательных требований или отклонение объекта от параметров;
- истек срок исполнения решения контрольного (надзорного) органа об устранении - нарушения обязательных требований (в установленных случаях);
- наступило событие, указанное в программе проверок;
- поступило поручение Президента РФ или Правительства РФ о проведении указанных мероприятий в отношении конкретных контролируемых лиц;

ФЗ от 31 июля 2020 г. №248 "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации".

В границах от 09 января 2024г. по 22 января 2024г. ответственному оператору необходимо подготовить акт о наличии нарушения по одному (или нескольких), пунктов и, при наличии таковых, - акт об оценке степени вреда в соответствии со ч. 3 ст. 7 Закона №248-ФЗ.

Акт (акты) передать для урегулирования инспектору Федеральной службой по Финансовому Мониторингу в соответствии с п. 5 ст. 18.1 Закона от 27.07.2006 №152-ФЗ.

На установление причин и ликвидацию последствий дано 10 рабочих дней, - приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 №187-ФЗ

Директор: А. Бортников

ПРИМЕРЫ УЛОВОК МОШЕННИКОВ

Мошенники направляют сообщение в мессенджере от имени органа государственной власти в виде вложения письма:

- На рисунке якобы **официальное обращение от УФСБ России по Московской области о голосовом согласии на сотрудничество с ФСБ России**, заверенное подписью и печатью руководителя, о голосовом согласии в сотрудничестве с органами государственной власти

ФСБ РОССИИ
Управление
Федеральной службы безопасности
Российской Федерации
по Московской области
(УФСБ России по Московской области)
ул.Большая Лубянка,д.2,г.Москва,107031

[redacted]

Согласие на сотрудничество

[redacted] дав голосовое согласие на сотрудничество с Федеральной Службой Безопасности Российской Федерации обязуется не разглашать сведений, составляющих государственную и служебные тайны, точно выполнять относящиеся к ней (нем) требования приказов, положений, инструкций по обеспечению режима секретности проводимых работ.

Об ответственности по закону разглашений сведений, составляющих государственную тайну, утрату документов, содержащие такие сведения, а также об ответсвенности за нарушения установленного режима секретности проводимых работ предупрежден (а).

Инструктаж провел [redacted]

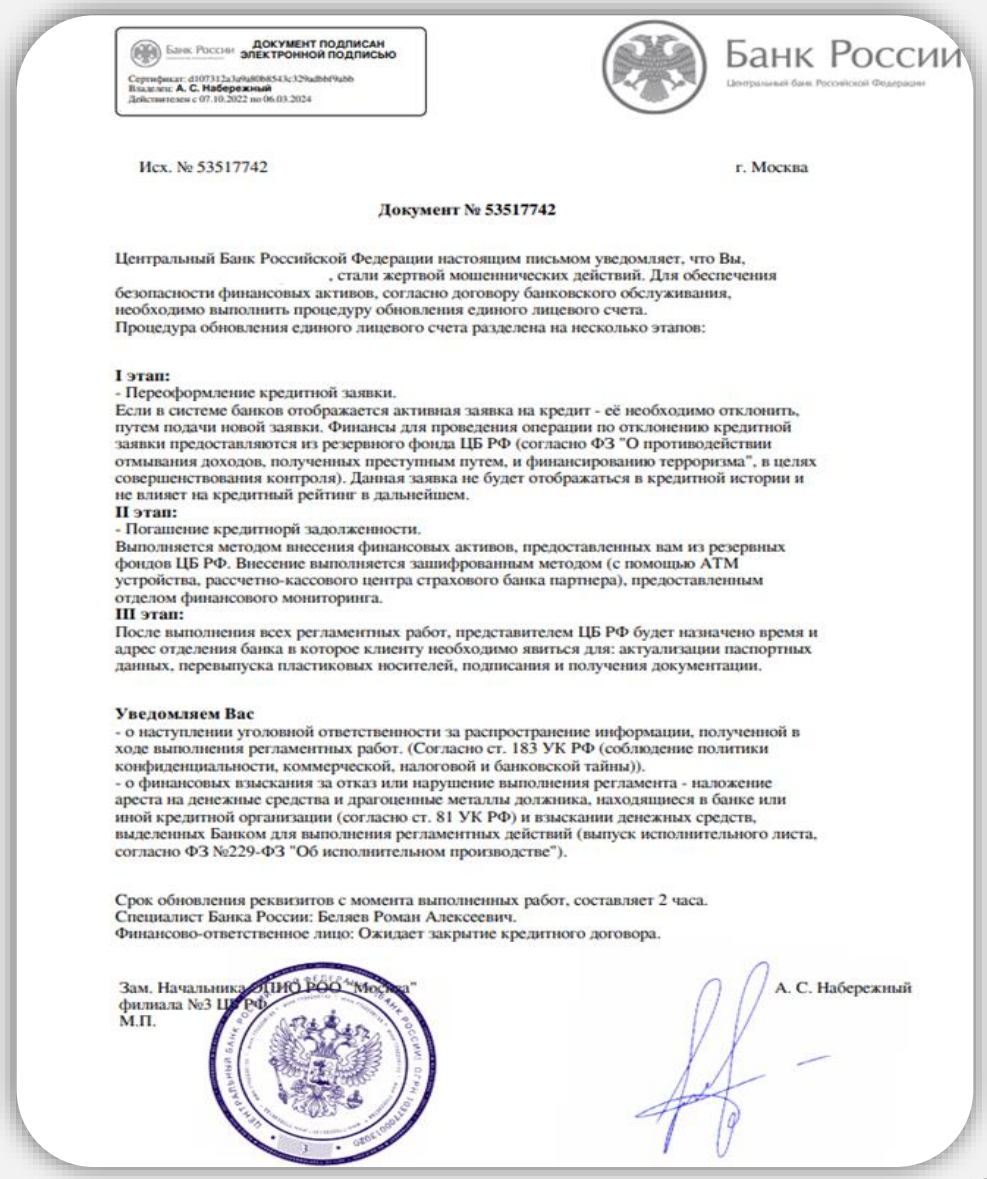
ст. следователь следственного отдела УФСБ

< 26 > сентября 2023 г.

ПРИМЕРЫ УЛОВОК МОШЕННИКОВ

Мошенники направляют сообщение в мессенджере от имени органа государственной власти в виде вложения письма:

- На рисунке **документ о необходимости проведения процедуры обновления единого лицевого счета якобы от Банка России**, заверенное подписью и печатью руководителя, о голосовом согласии в сотрудничестве с органами государственной власти



Банк России ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: d3073123a3a9a80b8543c329adbbf9abb
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 кредитиорй 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

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»...».

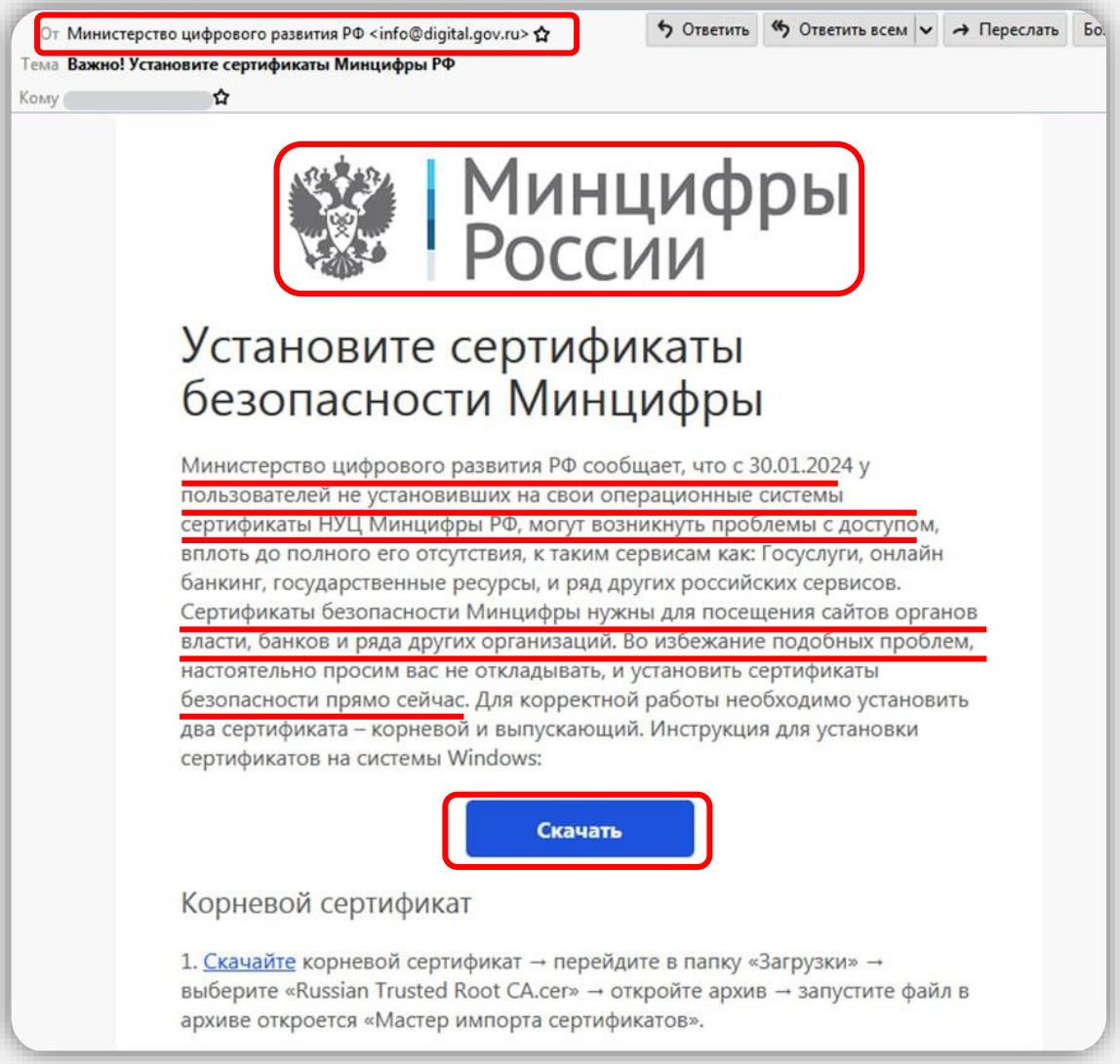
От 19.01.2024 № 240/91/208

«…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

ФАЛЬШИВЫЕ СЕРТИФИКАТЫ БЕЗОПАСНОСТИ ОТ «МИНЦИФРЫ»


От Министерство цифрового развития РФ <info@digital.gov.ru>
Ответить | Ответить всем | Переслать
Тема Важно! Установите сертификаты Минцифры РФ
Кому

Минцифры России

Установите сертификаты безопасности Минцифры

Министерство цифрового развития РФ сообщает, что с 30.01.2024 у пользователей не установивших на свои операционные системы сертификаты НУЦ Минцифры РФ, могут возникнуть проблемы с доступом, вплоть до полного его отсутствия, к таким сервисам как: Госуслуги, онлайн банкинг, государственные ресурсы, и ряд других российских сервисов. Сертификаты безопасности Минцифры нужны для посещения сайтов органов власти, банков и ряда других организаций. Во избежание подобных проблем, настоятельно просим вас не откладывать, и установить сертификаты безопасности прямо сейчас. Для корректной работы необходимо установить два сертификата – корневой и выпускающий. Инструкция для установки сертификатов на системы Windows:

Скачать

Корневой сертификат

1. Скачайте корневой сертификат → перейдите в папку «Загрузки» → выберите «Russian Trusted Root CA.cer» → откройте архив → запустите файл в архиве откроется «Мастер импорта сертификатов».

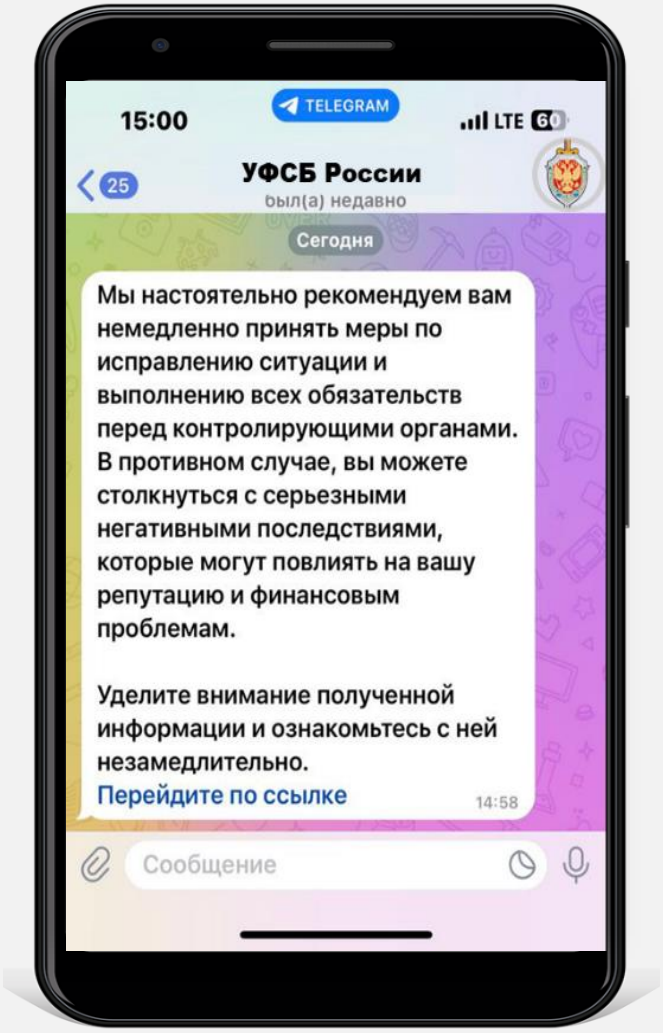
- С 25 января мошенники рассылают фишинговые письма, подменяя официальный электронный адрес Минцифры России. Официальный домен: **@minsvyaz.ru**
- Обращаем внимание на высокое качество подготовки текста фишингового письма (грамотность, стилистика, эмблема, оформление). Тематика обращения соответствует деятельности Минцифры России.
- Основные признаки фишинга – срочность и угрозы.
- Наличие вложения.

При переходе по ссылке происходит загрузка стилера MetaStealer (шпионское ПО, которое нацелено на кражу информации с устройства жертвы).

Рекомендации при получении подобного письма на рабочую почту

1. **Перешлите его на DITantifishing@mos.ru**
2. **Не переходите по ссылке/не открывайте вложение**
3. **Если перешли по ссылке, сообщите своему руководителю и в службу технической поддержки по тел.: 75555, +7(495)989-80-25**
4. **Если подобное письмо пришло на личную почту – удалите его**

ФИШИНГ ОТ ЛИЦА ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ



Мошенник пишет **сообщение от лица госоргана**

Переход по ссылке или открытие файла

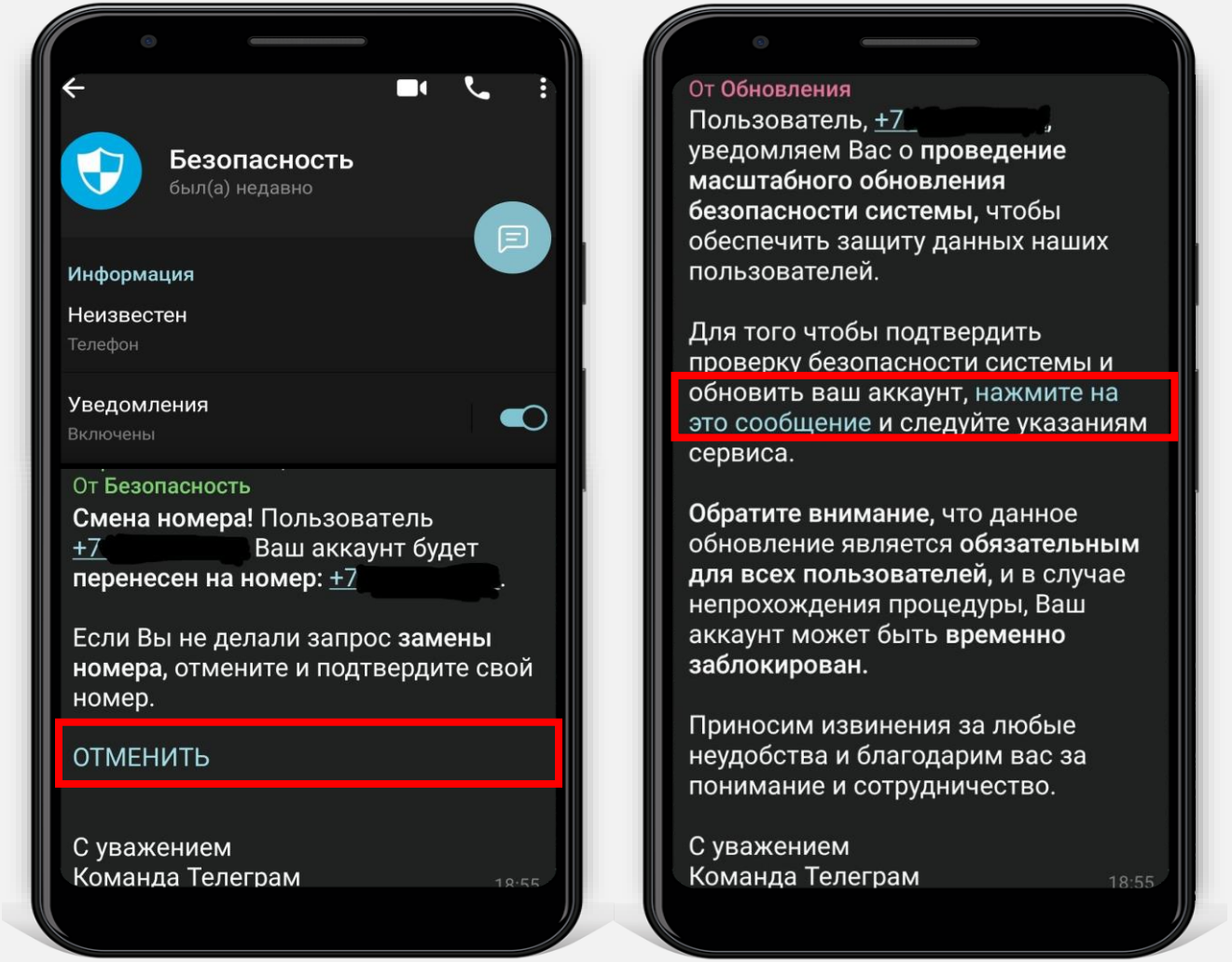
Происходит заражение устройства, злоумышленник получает контроль над устройством, а следовательно и к информации на нем

ФИШИНГ ОТ ЛИЦА ОРГАНА ГОСУДАРСТВЕННОЙ ВЛАСТИ

Важно помнить:

- **Уведомление гражданина** органы государственной власти осуществляют лично **исключительно в письменном виде и вручают лично**.
- Сотрудники органов государственной власти **никогда не присылают** гражданам копии своих **служебных удостоверений**.
- Органы государственной власти **не используют личные сбережения или кредитные средства граждан** для оказания помощи оперативным подразделениям в предупреждении и раскрытии преступлений.
- **Официальные телефоны** органов государственной власти используются **исключительно для приема информации** от граждан и организаций.

МОШЕННИКИ ДЕЙСТВУЮТ ПОД «МАСКОЙ» TELEGRAM

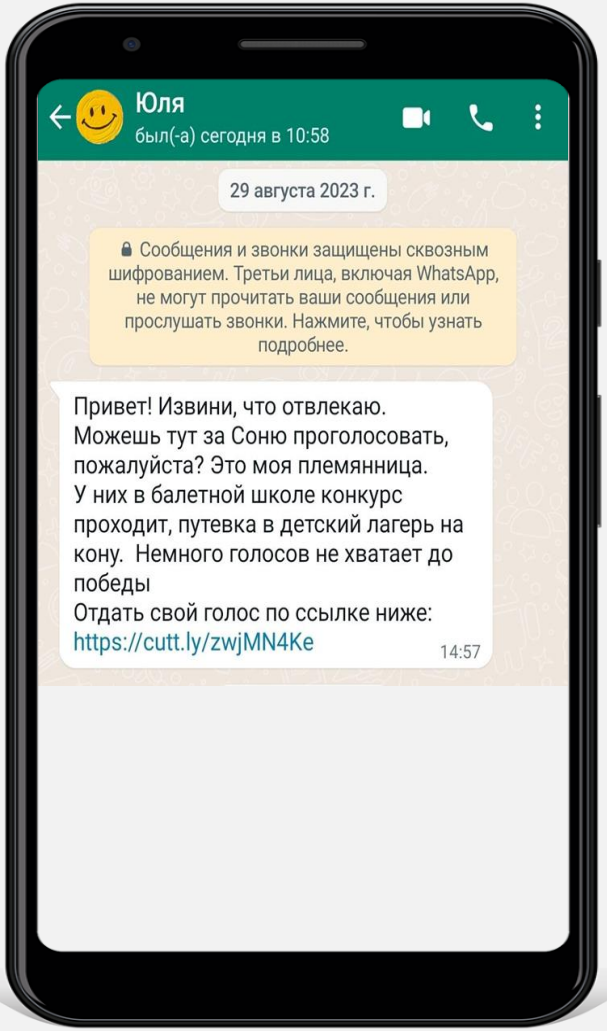


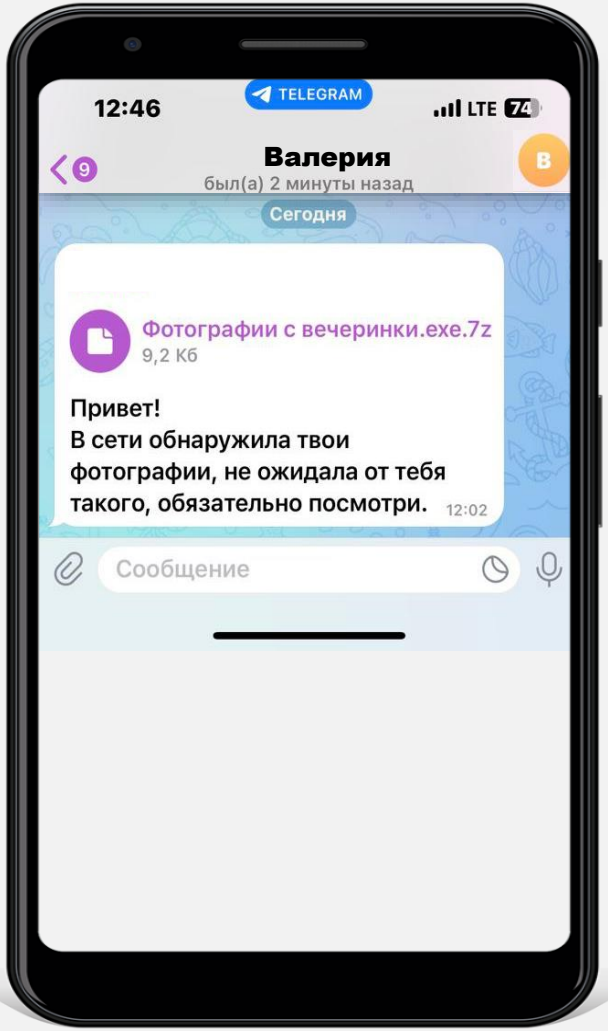
Получение **сообщения** якобы от **Команды Телеграм**

- **Сами ссылки спрятаны под текст** *(«Отменить», «Нажмите на сообщение» под текстом скрываются фишинговые ссылки)*
- **В сообщении побуждают к необдуманным действиям** *(например, обновить систему безопасности, отменить привязку другого номера к аккаунту, обновить аккаунт и т.д.*
- **Манипуляция страхом**

Перейдя по ссылке вы **теряете аккаунт** или происходит **заражение устройства**

ФИШИНГ ОТ ЗНАКОМОГО КОНТАКТА, КОТОРОГО ВЗЛОМАЛИ





Сообщение:

- с просьбой поучаствовать в опросе или проголосовать за него в конкурсе (переход по ссылке)
- с вложенным файлом

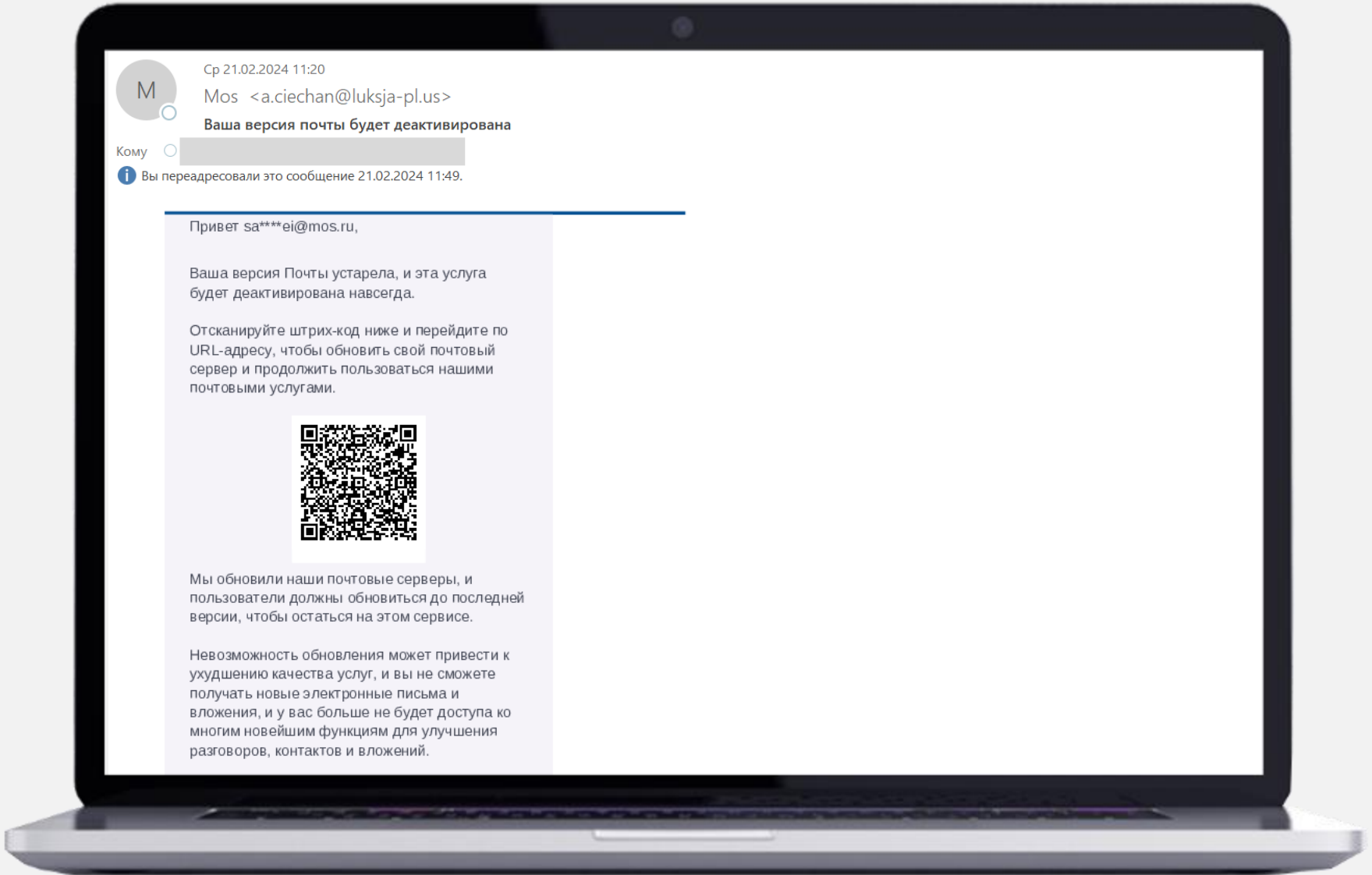
Открытие файла / переход по ссылке

Происходит заражение устройства, а следовательно потеря контроля над ним.

2.

- ФИШИНГ ПО ПОЧТЕ

ПРИМЕРЫ ФИШИНГОВЫХ ПИСЕМ В ПОЧТЕ

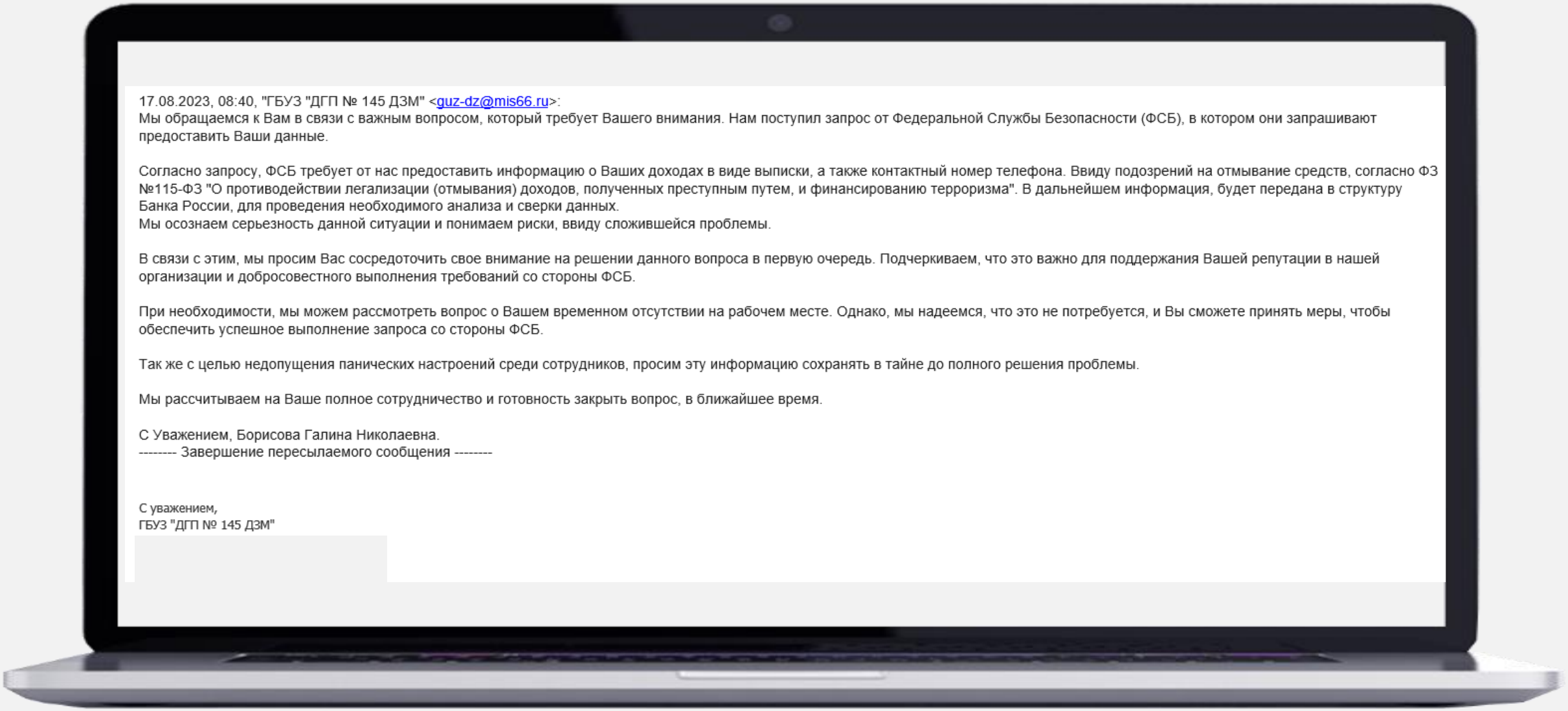


Если отправитель почты неизвестен, в письме присутствуют признаки манипуляции, у вас запрашивают пароль от лица техподдержки и т.д.:

- не переходите по ссылкам,
- не сообщайте пароль,
- не запускайте вложения
- перешлите сомнительное письмо в службу безопасности по адресу: DITantifishing@mos.ru

ПРИМЕРЫ ФИШИНГОВЫХ ПИСЕМ В ПОЧТЕ

ДИТ



17.08.2023, 08:40, "ГБУЗ "ДГП № 145 ДЗМ" <guz-dz@mis66.ru>:
Мы обращаемся к Вам в связи с важным вопросом, который требует Вашего внимания. Нам поступил запрос от Федеральной Службы Безопасности (ФСБ), в котором они запрашивают предоставить Ваши данные.

Согласно запросу, ФСБ требует от нас предоставить информацию о Ваших доходах в виде выписки, а также контактный номер телефона. Ввиду подозрений на отмывание средств, согласно ФЗ №115-ФЗ "О противодействии легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма". В дальнейшем информация, будет передана в структуру Банка России, для проведения необходимого анализа и сверки данных.
Мы осознаем серьезность данной ситуации и понимаем риски, ввиду сложившейся проблемы.

В связи с этим, мы просим Вас сосредоточить свое внимание на решении данного вопроса в первую очередь. Подчеркиваем, что это важно для поддержания Вашей репутации в нашей организации и добросовестного выполнения требований со стороны ФСБ.

При необходимости, мы можем рассмотреть вопрос о Вашем временном отсутствии на рабочем месте. Однако, мы надеемся, что это не потребуется, и Вы сможете принять меры, чтобы обеспечить успешное выполнение запроса со стороны ФСБ.

Так же с целью недопущения панических настроений среди сотрудников, просим эту информацию сохранять в тайне до полного решения проблемы.

Мы рассчитываем на Ваше полное сотрудничество и готовность закрыть вопрос, в ближайшее время.

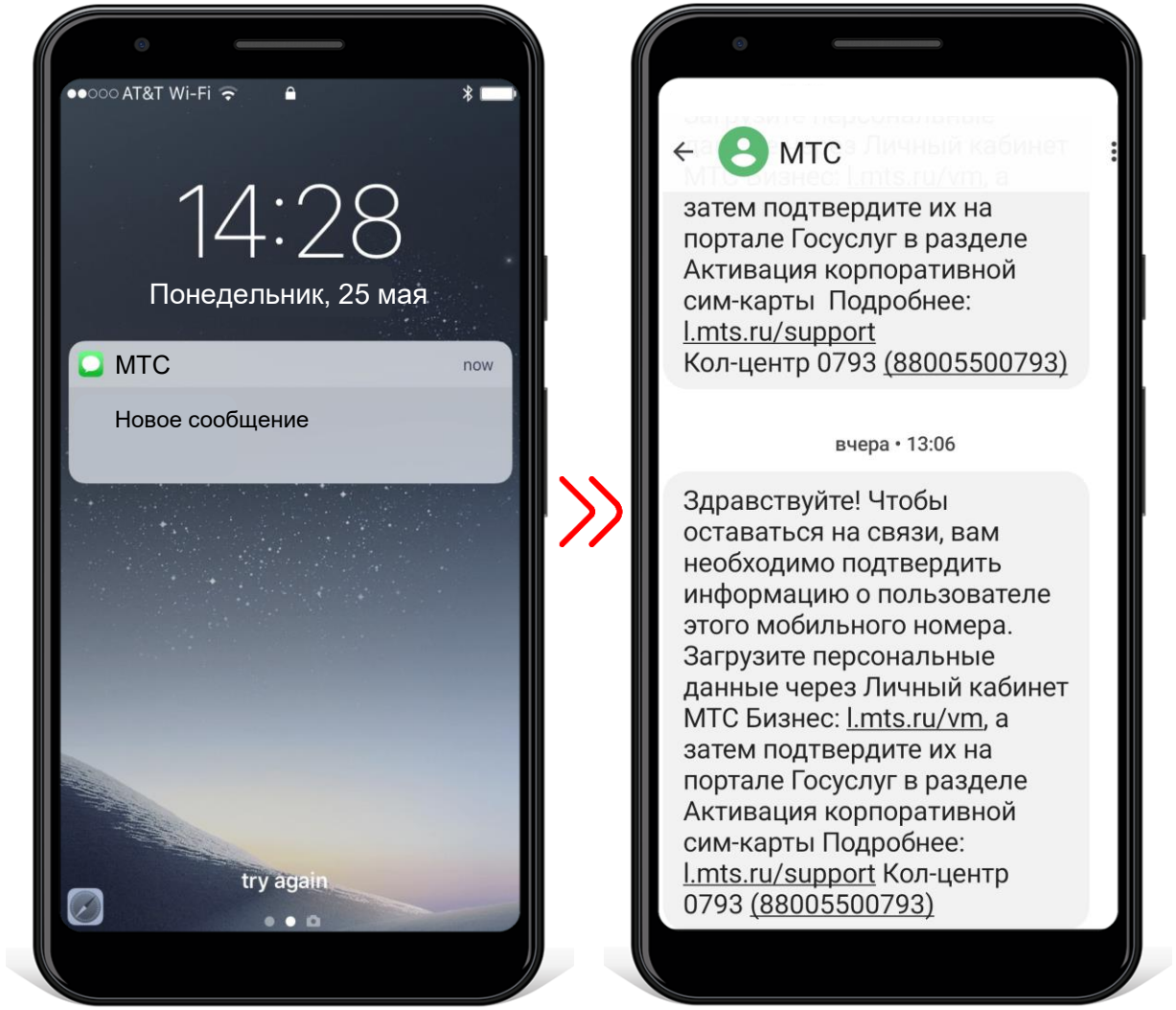
С Уважением, Борисова Галина Николаевна.
-------- Завершение пересылаемого сообщения --------

С уважением,
ГБУЗ "ДГП № 145 ДЗМ"

3.

- ФИШИНГ ОТ ИМЕНИ ОПЕРАТОРА СВЯЗИ ДЛЯ ВЗЛОМА «ГОСУСЛУГ»

ФИШИНГ ОТ ИМЕНИ ОПЕРАТОРА СВЯЗИ ДЛЯ ВЗЛОМА «ГОСУСЛУГ»



Злоумышленники **от имени оператора связи** (под предлогом продления мобильного номера) **совершают звонки, направляют электронные письма или push-уведомления.**

Они просят **подтвердить паспортные данные,** для этого:

- Направляют **фишинговую ссылку**, с которой вы переходите на **фиктивную страницу Госуслуг;**
- **Направляют код и** просят его назвать или вписать.

Перейдя по ссылке или сообщив код, **вы теряете доступ к личному кабинету Госуслуг**

МОШЕННИКИ ВЗЛОМАЛИ ЛИЧНЫЙ КАБИНЕТ НА САЙТЕ «ГОСУСЛУГ». ЧТО ДЕЛАТЬ?

ДИТ

Стандартная/ упрощенная учетная запись – онлайн

Онлайн на Госуслугах — если есть доступ к телефону и почте из личного кабинета

(мошенники НЕ поменяли почту и пароль в вашем личном кабинете)

1. На странице ввода логина и пароля нажмите «Восстановить»
2. Укажите номер телефона или электронную почту, а также данные одного из документов:
   - паспорт
   - ИНН
   - СНИЛС
3. Ответьте на контрольный вопрос, если он был установлен
4. Перейдите по ссылке из письма в электронной почте или введите код из смс.
5. Придумайте новый пароль и нажмите «Сохранить».

Стандартная/ упрощенная учетная запись – онлайн

Онлайн через банк — если нет доступа к телефону и почте из личного кабинета

(мошенники поменяли почту и пароль в вашем личном кабинете)

1. Посмотрите список банков, в которых можно онлайн восстановить доступ к порталу.
2. Если вы являетесь клиентом одного из них, зайдите в свой личный кабинет на сайте или в приложении, найдите сервис «Регистрация на «Госуслугах» и следуйте инструкциям.
3. Новый пароль от аккаунта придет на номер телефона, который вы указали в банке как основной.
4. Даже если мошенники успели заменить его в «Госуслугах» на свой, код для входа получите именно вы.

Подтвержденная учетная запись – офлайн

Лично в центре обслуживания — если нет доступа к телефону и почте из личного кабинета

(мошенники поменяли или установили контрольный вопрос и иные данные)

1. Выберите удобный центр обслуживания. Нажмите на фильтр (значок, похожий на воронку), выберите «Восстановление доступа».
2. Возьмите с собой паспорт и СНИЛС
3. Предъявите документы и попросите оператора восстановить пароль от Госуслуг
4. Проверьте, какой номер телефона привязан к профилю. Если указан не ваш, сразу замените его.
5. При первом входе на Госуслуги с новым паролем укажите в качестве логина СНИЛС
6. Смените полученный пароль.

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ЛИЧНОГО КАБИНЕТА ПОСЛЕ ЕГО ВОССТАНОВЛЕНИЯ?

ДИТ

1 В разделе «Настройка учетной записи»

- Проверьте телефон и почту, если там указаны неизвестные номер или адрес, сделайте скриншот — эти данные помогут в поиске преступников
- Поменяйте телефон и электронную почту

2 В разделе «Безопасность» настройте

- Вход с подтверждением по смс в дополнение к паролю
- Оповещение на электронную почту после входа
- Восстановление доступа контрольным вопросом

3 В разделе Безопасность» в подразделе «Действия в системе»

- Проверьте, не было ли подозрительных действий в учётной записи
- При необходимости обратитесь в службу поддержки
- При необходимости сделайте фото или скриншот — возможно, эта информация вам пригодится

4 В разделе «Согласия и доверенности» в подразделе «Разрешения»

- Отзовите разрешения, которые вы не выдавали
- Узнаете, какие ведомства запрашивали вашу личную информацию
- При необходимости сделайте фото или скриншот — возможно, эта информация вам пригодится

5 Проверьте информацию о ранее поданных заявлениях

- Перейдите в личный кабинет в Уведомления → Заявления
- Это поможет выявить, какие действия хотели совершить или совершили мошенники от вашего имени

6 Подайте заявление в МВД России

- Обратитесь в подразделение МВД России
- Расскажите о взломе и приведите всю информацию, которую знаете

ДОПОЛНИТЕЛЬНЫЕ МЕРЫ БЕЗОПАСНОСТИ

ДИТ

Используйте уникальный логин и пароль, которые не встречаются на других сайтах

Никому не сообщайте ответ на контрольный вопрос и коды из смс, в том числе приходящие от отправителя gosuslugi и с номера 0919

Внимательно проверяйте адрес сайта https://www.gosuslugi.ru. Проверяйте, чтобы в адресной строке не было похожих написаний вроде gossuslugi, gos.uslugi, gosuclugi и т.д.

Не переходите по подозрительным ссылкам. Ссылки от Госуслуг обычно ведут в личный кабинет, на конкретную услугу и сайты ведомств

Не открывайте присланные файлы, если не уверены в отправителе. Письма от Госуслуг приходят с адресов no-reply@gosuslugi.ru или no-reply@pos.gosuslugi.ru

Устанавливайте официальные приложения. Приложение «Госуслуги» можно скачать в RuStore, Google Play, App Store и AppGallery

ВСЕГДА НА СВЯЗИ!

Департамент
информационных
технологий
города Москвы

www.dit.mos.ru