



**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ ДАГЕСТАН
(МИНОБРНАУКИ РД)**

367001, г. Махачкала, ул. Даниялова, д. 32, тел.: +7(8722) 67-18-48, e-mail: dagminobr@e-dag.ru

04.10.2024 № 06-15546/09-18/24

**Руководителям муниципальных
органов управления образования**

**Руководителям образовательных
организаций подведомственных
Минобрнауки РД**

**Руководителям образовательных
организаций среднего
профессионального образования**

В соответствии с письмом Отделения Южного главного управления Центрального банка Российской Федерации – Национальный банк по Республике Дагестан от 27 сентября 2024 г. № Т382-4/3034 об участии в информационной кампании по киберграмотности «Клади трубку», направленной на распознавание телефонных мошенников, просвещения несовершеннолетних обучающихся о преступлениях в информационно-телекоммуникационной сети «Интернет» (далее соответственно – Национальный банк по РД, Акция «Клади трубку», сеть «Интернет»), Министерство образования и науки Республики Дагестан сообщает.

В связи с тем, что на сегодняшний день тема финансовой кибербезопасности остается одной из самых актуальных в профилактике и пресечении мошеннических действий, краж с использованием информационно-телекоммуникационных технологий, Национальным банком по РД организовано проведение Акции «Клади трубку».

С целью профилактики правонарушений и преступлений в сети «Интернет» среди несовершеннолетних, повышения правовой и финансовой грамотности по использованию информационных технологий просим обеспечить в период с 3 по 31 октября 2024 г. проведение в организованных в рамках Акции «Клади трубку» Национальным банком по РД мероприятий:

– Акции «Клади трубку» в соответствии с Концепцией проведения Акции по киберграмотности «Клади трубку» согласно приложению № 1 к настоящему письму;

– Урока на тему киберграмотности по Сценарию согласно приложению № 2 к настоящему письму;

– Классного часа на тему кибербезопасности с использованием презентации и подстрочника согласно приложению № 3 к настоящему письму;

– Трансляции по радио во время перемен между занятиями аудиороликов по финансовой грамотности согласно приложению № 4 к настоящему письму;

– Трансляции короткометражных видеороликов на экранах мониторов в коридорах учебных заведений, классах (при наличии возможности) согласно приложению № 5 к настоящему письму.

Кроме того, просим разместить на официальных страницах образовательных организаций в сети «Интернет», а также на стендах при входе и фойе образовательных организаций памятки согласно приложению № 6 к настоящему письму.

Информация о проведенных мероприятиях и проделанной работе просим в срок до 1 ноября 2024 г. внести по ссылке: <https://forms.yandex.ru/u/66dea7465d2a068e7f5151e0/>.

Приложение: в электронном виде.

Министр

Я.Г. Бучаев

З.Д. Гаджирагимова
8(8722)67-84-51

Приложение 1
к письму Отделения-НБ Республика
Дагестан
«Об участии в ИК «Клади трубку»

КОНЦЕПЦИЯ проведения акции по киберграмотности «Клади трубку».

Период проведения акции: 1 - 31 октября 2024 года.

Наименование: акция «Клади трубку».

Организаторы акции: Отделение-НБ Республика Дагестан,
Министерство образования и науки Республики Дагестан.

Место проведения: образовательные организации республики.

Цель акции: научить детей и молодежь распознавать телефонных мошенников, рассказать о преступных схемах, раскрыть ключевые индикаторы, которые сигнализируют о мошенничестве и необходимости прервать разговор.

Участники акции: учащиеся образовательных организаций республики в возрасте 14-17 лет.

Механизм и этапы реализации акции.

Рекомендуется в течение акции:

- организовать трансляцию видеороликов и аудиосообщений (сообщения для граждан) на территории образовательной организации;
- размещение на досках объявления, входных зонах плакаты, листовки по киберграмотности.

1 этап с 1 по 18 октября 2024 года: проведение урока по киберграмотности «Клади трубку» для учеников старших классов (приложение: сценарий урока, презентация, подстрочник к презентации);

2 этап с 21 по 25 октября 2024 года: проведение челленджа интернет-роликов или фотографий на тему «Клади трубку» с размещением в социальных сетях с хэштегом: **#КладиТрубку82**.

28 - 31 октября 2024 года: заполнение отчета в Яндекс-форме (приложение: ссылка на Яндекс-форму).

Пункты отчета¹:

- «Количество точек трансляции видеороликов в учебном заведении (число)»;
- «Организована трансляции аудиороликов (да/нет)»;
- «Количество проведенных уроков по киберграмотности (число)»;

¹ Предварительно при заполнении отчета необходимо выбрать название региона, название муниципального образования, а также указать адрес образовательной организации.

- «Количество слушателей урока по киберграмотности (число)»;
- «Суммарное количество просмотров опубликованных работ (видеоролика или фотографий) в социальных сетях в рамках челленджа (число)»;
- «Ссылки на опубликованный материал (ссылки)».

1 - 5 ноября 2024 года: направление отчета.

6 - 7 ноября 2024 года: подведение итогов акции, согласно заполненной Яндекс-форме. По итогам опубликованных работ определены три победителя, которые набрали максимальное количество просмотров в социальной сети(ях).

8 ноября 2024 года: объявление итогов акции. Направление Отделением-НБ Республика Дагестан информации об итогах в Министерство образования и науки Республика Дагестан.

Приложение 2
к письму Отделения-НБ Республика
Дагестан
«Об участии в ИК «Клади трубку»

СЦЕНАРИЙ

урока на тему киберграмотности для проведения акции «Клади трубку»

1. Описание урока.

Урок проводится по материалам презентации: акция «Клади трубку».

Презентация с подстрочником является дополнительным материалом для организации занятий по киберграмотности, цель которых формирование навыков противодействия мошенникам и грамотного финансового поведения.

Задачи:

- рассказать и рассмотреть на примерах виды кибермошенничества;
- научиться распознавать мошенников и определять причины, по которым люди становятся жертвами кибермошенников.

Форма проведения: урок/лекция с элементами симуляции.

Методы и приемы: введение базовых понятий и анализ конкретных кейсов/ситуаций.

Продолжительность: 45 минут.

Количество участников: не ограничено.

Возраст участников: 14+.

Требования к лектору: Роль лектора выполняет сотрудник образовательной организации (педагог, учитель), изучивший методические рекомендации и инструкцию к уроку. Лектор может не обладать специальными знаниями по финансовой грамотности.

Оборудование, материалы: интерактивная доска/проектор, ноутбук, презентация с подстрочником.

2. План урока:

№	Название этапа урока	Время	Комментарии
1	Вводная часть	3 мин	Введение в тему. Объяснение цели урока. Рассказ о количестве ущерба, который приносят кибермошенники. Слайд 1 (подстрочник).
2	Объяснение материала: распространенные схемы кибермошенников	10 мин	Рассказ о распространенных схемах телефонных мошенников. Слайды 2-4 (подстрочник).
3	Объяснение материала: виды социальной инженерии	10 мин	Рассказ об основных видах социальной инженерии, формулах их «успеха». Слайды 5-7 (подстрочник).
4	Уловки мошенников, примеры «фальшивок»	5 мин	Примеры «фальшивок»: документы, сайты, новостной фишинг Слайды 8-10 (подстрочник).
5	Разъяснение основных правил киберграмотного поведения	10 мин	Общие правила поведения с кибермошенниками и как противостоять телефонным мошенникам.

			Слайды 11-13 (подстрочник).
6	Закрепление изученного материала. Подведение итогов урока.	7 мин	Вопросы-ответы.

Слайд 0

ЗАСТАВКА

Слайд 1

Основным инструментом злоумышленников для хищения денег остается использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит деньги или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Проблема мошенничества актуальна как в отношении физических, так и в отношении юридических лиц.

На протяжении последних четырех лет Банк России фиксирует ежегодное увеличение объема операций, совершенных без добровольного согласия клиентов. В 2023 году злоумышленники похитили 15,8 млрд руб. По сравнению с 2022 годом объем похищенных денег вырос более чем на 11,4 %. Количество мошеннических операций увеличилось на 33% и превысило 1,1 млн.

В 2023 году: банки отразили 34,8 млн попыток кибермошенников похитить деньги у граждан, сохранив 5,8 трлн рублей.

В 2023 году количество мошеннических операций с использованием платежных карт было самым высоким среди остальных типов операций. Использование злоумышленниками чувствительных данных увеличивает риск хищений как собственных накоплений граждан, так и полученных под влиянием мошенников кредитных средств.

Слайд 2

Телефонный звонок – ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам. Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Приведем некоторые распространенные способы обмана:

1. **Якобы сотрудник Пенсионного фонда, соцслужбы.** Мошенники сообщают, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда. Причем для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.
2. **Якобы сотрудник поликлиники, аптеки, медицинского центра.** Мошенники соотносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо

срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить звонящему.

Слайд 3

3. **Якобы сотрудник банка** (как правило, представителя службы безопасности). Сценарии могут быть разные: от классического «с вашей карты пытаются перевести деньги» до пугающего «по карте замечены подозрительные операции, и она заблокирована». В любом случае итогом будет просьба сообщить информацию по карте или счету, код из СМС-сообщения.
4. **Якобы друг, родственник.** Мошенник может представиться родственником/другом, попавшим в неприятную ситуацию, или ее случайным свидетелем, а также представителем правоохранительных органов, который готов помочь гражданину с решением проблемы. Схема довольно старая, но мошенники продолжают ею пользоваться, так как страх за близкого человека – это очень сильная эмоция.

Слайд 4

Мошенники очень часто представляются якобы сотрудниками Центрального банка (Банка России). Гражданам звонят и от имени Центробанка сообщают, что по их карте зафиксирована подозрительная активность: пытаются перевести все деньги за рубеж. Чтобы сохранить свои деньги и подтвердить, что это не сам человек совершает данную операцию, ему необходимо открыть в Центробанке «защищенный/безопасный/специальный» личный счет. Для этого уточняют паспортные данные, просят подтвердить данные по счету/карте, а для открытия счета просят подтвердить небольшой перевод на этот счет, который Центробанк якобы совершает для своих клиентов, то есть сообщить код из СМС. Следует помнить, что Банк России не работает с физическими лицами. При поступлении телефонного звонка от Банка России немедленно прервите разговор.

Также иногда злоумышленники представляются сотрудниками правоохранительных органов. Такие мошенники долго и подробно рассказывают об обстоятельствах уголовного дела, участником которого, по их словам, гражданин является. Далее для уточнения информации они просят сообщить личную и финансовую информацию. Это и является признаком того, что гражданин разговаривает с мошенником: правоохранительные органы не просят назвать по телефону финансовую информацию. Помните, что настоящие сотрудники полиции никогда не запрашивают личные и финансовые данные по телефону.

Слайд 5

Социальная инженерия – введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа (банковские карты, онлайн-банк) или побуждения владельцев самостоятельно совершить перевод денежных средств с целью их хищения.

Основные проявления социальной инженерии:

1. Обман или злоупотребление доверием (например, мошенники представляются сотрудниками банков, правоохранительных органов или родственниками).
2. Психологическое давление.
3. Манипулирование.

Действительно, мошенники оказывают психологическое давление (торопят, сознательно пугают или, наоборот, приводят в состояние эйфории) и, используя вызванные положительные или отрицательные эмоции, манипулируют действиями граждан. Существуют различные методы социальной инженерии. Телефонное мошенничество – это один из основных инструментов, которым активно пользуются злоумышленники.

Слайд 6

В чем заключается «успех» мошенников?

Формула «успеха» телефонных мошенников: неожиданность + сильные эмоции (положительные и отрицательные) + психологическое давление и создание паники + актуальная тема = вы готовы сделать все, что от вас просят мошенники (перевести деньги, совершить финансовые операции, сообщить личную или финансовую информацию).

Распространенные мошеннические схемы, а также способы противодействия им Банк России публикует на своем официальном сайте в разделе «Противодействие мошенническим практикам».

Слайд 7

Как действуют мошенники, что человек, отбросив все свои знания, все равно идет у них на поводу?

Прежде всего злоумышленникам играет на руку эффект неожиданности. Застав Вас врасплох, они подключают к действию эмоции:

Мошенники воздействуют на основные базовые эмоции. Задача киберпреступников – вывести человека из спокойного состояния и отключить у него критическое мышление.

Положительные: радость, желание быстрее получить деньги или выгоду (как правило, такие эмоции человек испытывает после таких фраз, как: «Вам положены социальные выплаты», «Вы выиграли крупную сумму денег» и другие похожие истории).

Отрицательные: страх, испуг, желание помочь, спасти или родного человека, или свои сбережения (эти эмоции проявляются у человека после таких фраз, как: «Ваш сын попал в аварию», «С Вашей карты пытаются украсть деньги»).

Они активируют базовые эмоции, обеспечивая быструю и необдуманную реакцию жертвы.

Слайд 8

Одной из распространенных мошеннических схем является ситуация, когда мошенники представляются сотрудниками Банка России или правоохранительных органов. С целью сохранения денежных средств они настаивают на выполнении процедуры обновления единого лицевого счета в Банке России. Чтобы гражданин окончательно поверил в реальность лжеситуации, мошенники могут прислать целый пакет якобы подтверждающих документов: сканы официальных документов с подписями и печатями, фотографии удостоверений сотрудников и другие документы на официальных бланках органов государственной власти. К сожалению, такие документы могут содержать фамилии реальных работников — эти сведения злоумышленники могут брать с сайта Банка России (или с сайта той организации, сотрудниками которой они представляются). Высылая фальшивое удостоверение или документы, они надеются убедить человека в правдоподобности своих мошеннических действий, чтобы в дальнейшем лишить его денег или оформить на него кредит. На самом деле сотрудники Банка России не звонят людям и не направляют никому копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом.

Слайд 9

Еще один вид мошенничества — это фишинг. Злоумышленники подделывают популярные сайты (к примеру, органов власти и различных ведомств). Аферисты также подделывают сайты известных магазинов, маркетплейсов, туристических компаний и др. Например, на слайде представлен сайт, замаскированный под официальный сайт «Госуслуги». Несмотря на то что внешне он очень похож на настоящий, при внимательном рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена. Настоящий сайт «Госуслуги», а также официальные сайты финансовых организаций в популярных поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Слайд 10

Заметьте, что тематика фишинговых сайтов, как и сценарии телефонных звонков, также соответствует актуальным событиям: когда основной новостной повесткой была новая коронавирусная инфекция, злоумышленники всячески использовали ее в качестве поводов для выманивания денег у граждан. Для чего мошенники создают фишинговые сайты? Имитируя интернет-ресурсы популярных компаний, они рассчитывают, что пользователи не заметят подделку и оставят на поддельной фальшивой странице важную информацию: личные или финансовые данные, логин и пароль, контактные сведения (номер телефона и электронную почту). Заполучив чувствительную информацию, мошенникам будет легче обмануть человека.

Слайд 11

Существуют общие правила поведения с кибермошенниками. Следуя им, вы сможете себя обезопасить:

- не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с обратной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

- установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

- не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум – быть поводом для мошенников активизировать против вас мошенническую схему;

- не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;

- заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получают доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

Слайд 12

В случае если вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, – вы рискуете попасть на мошенников. Чтобы связаться с банком, самостоятельно наберите номер, указанный на обратной стороне вашей банковской карты или на официальном сайте кредитной организации.

Для того чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также подтверждающий код из СМС) – это, как правило, бесплатно. Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (Яндекс, Mail.ru), помеченными цветным кружком с галочкой.

Слайд 13

Как противостоять телефонным мошенникам?

Ни в коем случае не отвечайте на звонки с незнакомых номеров. Как правило, если вам звонят с работы или из другой организации, от которой вы ожидаете звонка, вам дополнительно напишут СМС-сообщение или сообщение в мессенджере. Никогда не перезванивайте по незнакомым вам номерам.

Если разговор касается финансовых вопросов, не продолжайте разговор и положите трубку. Сотрудники банков или правоохранительных органов не запрашивают Ваши личные и финансовые данные по телефону.

Не торопитесь принимать решение, ведь мошенники добиваются именно того, чтобы вы приняли быстрое и необдуманное решение. Они используют методы социальной инженерии: торопят Вас, пугают, создают чувство паники. Не стоит поддаваться такому давлению: проверьте информацию в Интернете или обратитесь за помощью к близким родственникам.

Прежде чем принять какое-то решение, связанное с финансами, позвоните близкому человеку, в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий. Важно получить подтверждение информации именно из официального источника, контактные номера при этом берите из своей записной книжки или с официальных сайтов организаций.

Не торопитесь принимать решение: всегда лучше проконсультироваться у специалиста, которому Вы доверяете, или посоветоваться с близкими и родственниками.

Будьте бдительны и оставайтесь в безопасности!

Будь умней телефонных
мошенников!

Клади
трубку



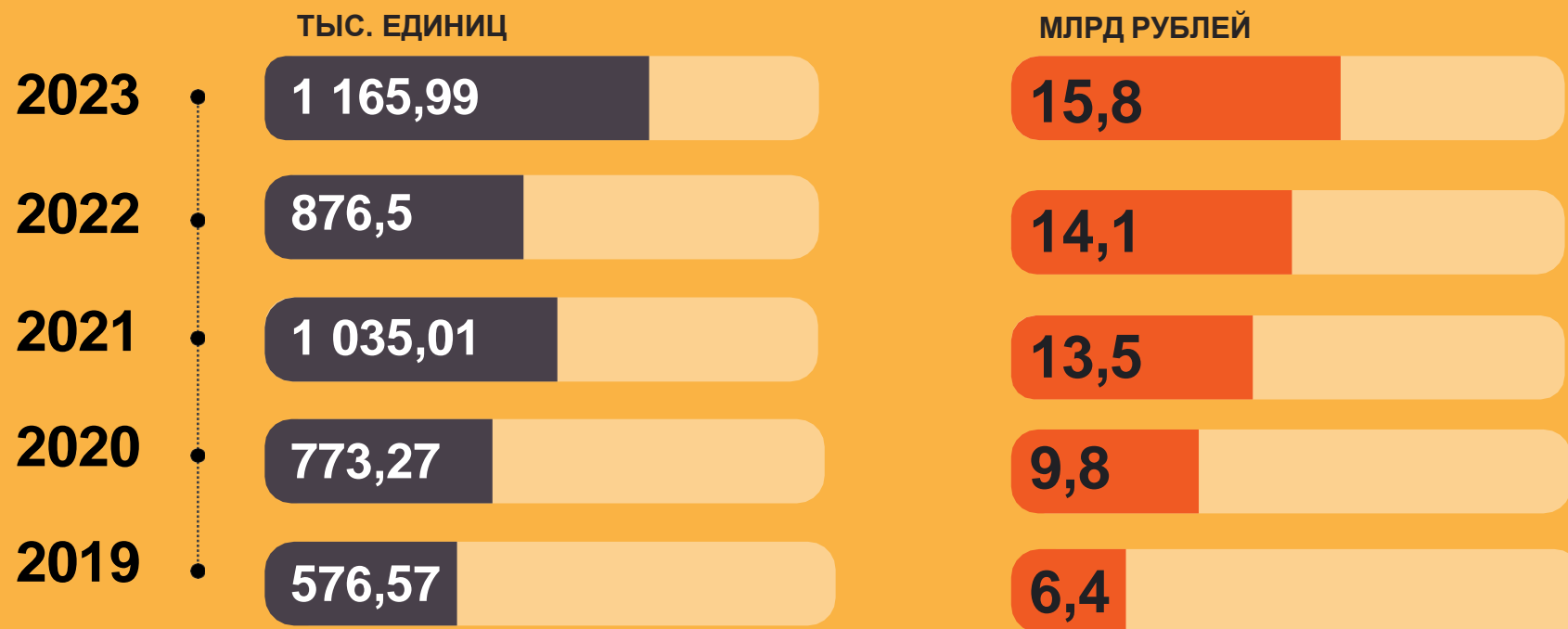
Без разговоров





Банк России

КИБЕРМОШЕННИЧЕСТВО: КОЛИЧЕСТВО ОПЕРАЦИЙ И УЩЕРБ



В 2023 году банки предотвратили 34,8 млн
мошеннических операций на 5,8 трлн рублей

ФИЗИЧЕСКИЕ И ЮРИДИЧЕСКИЕ ЛИЦА





ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК
ПЕНСИОННОГО ФОНДА
(СОЦИАЛЬНОЙ СЛУЖБЫ)»

«Вам положена социальная выплата по приказу Президента РФ»

Негосударственный пенсионный фонд «Незабудка» готов в качестве поддержки пенсионеров перевести на ваш счет...»



«МЕДИЦИНСКИЙ
РАБОТНИК»

«Вы сдавали у нас анализы. По их результатам вам требуется лечение»

«В нашей аптеке появилось дефицитное лекарство. Вам положена скидка»



ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК
БАНКА»

«С вашей карты пытаются перевести деньги»

«Ваша карта (счет) заблокирована»

«По карте зафиксирована подозрительная операция»



«ДРУГ,
РОДСТВЕННИК»

«Ваш сын попал в аварию, ему срочно требуется дорогостоящее лекарство»

«Ваш сын только что в результате ДТП сбил человека. Я готов помочь избежать наказания»



ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК
ЦЕНТРОБАНКА
(БАНКА РОССИИ)»

«По вашей карте зафиксирована сомнительная операция. Для сохранности денег вам нужно перевести их на «безопасный» («специальный») счет в Центробанке»



«ПРЕДСТАВИТЕЛЬ
ПРАВООХРАНИТЕЛЬНЫХ
ОРГАНОВ
(МВД, ФСБ, СК РФ)»

«Следователь Следственного комитета. Вы являетесь свидетелем по уголовному делу»
«Иванов В.В., капитан полиции. По вашему паспорту оформлен кредит и указана ваша карта. Нам необходимо уточнить ее реквизиты»



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – ЗЛО

Телефон — основной инструмент мошенников. Они обычно используют приемы и методы социальной инженерии

- 1 обман или злоупотребление доверием
- 2 психологическое давление
- 3 манипулирование



Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для хищения денег



Банк России

ФОРМУЛА УСПЕХА ТЕЛЕФОННЫХ МОШЕННИКОВ



эффект
неожиданности

+



яркие
эмоции

+



психологическое
давление, паника

+



актуальная
тема

Увы, мы готовы сделать **ВСЁ**,
что просят от нас мошенники



ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

положительные

- радость
- надежда
- желание получить деньги

«Вы выиграли крупную сумму денег»
«Вам положены социальные выплаты»
«Пенсионный фонд рад сообщить вам
о перерасчете вашей пенсии,
вам положена выплата в размере...»



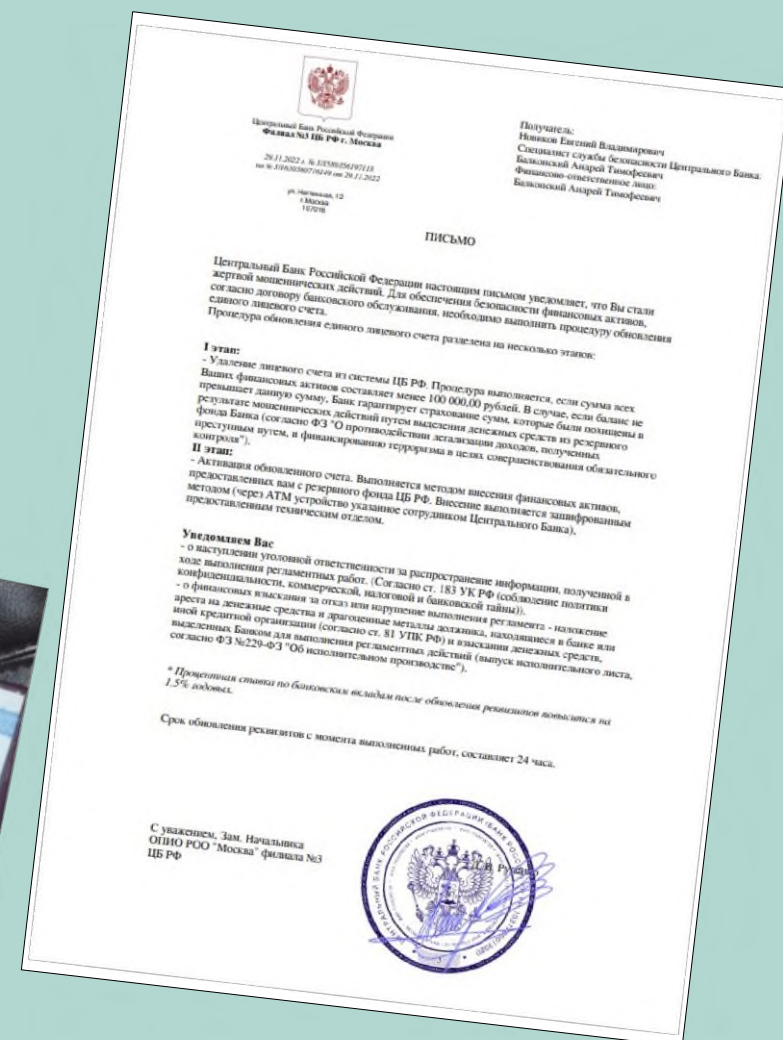
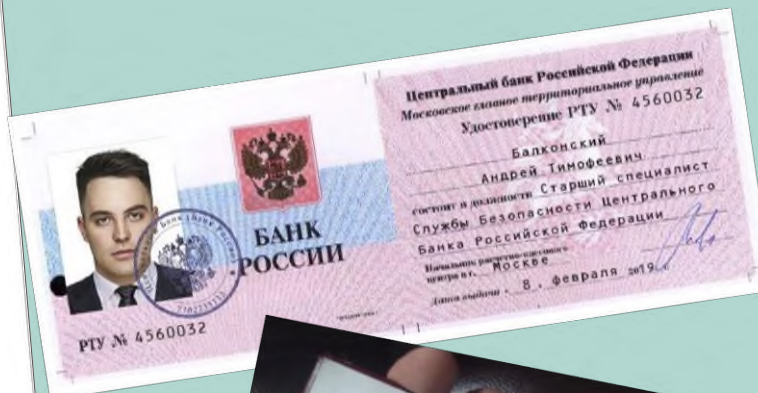
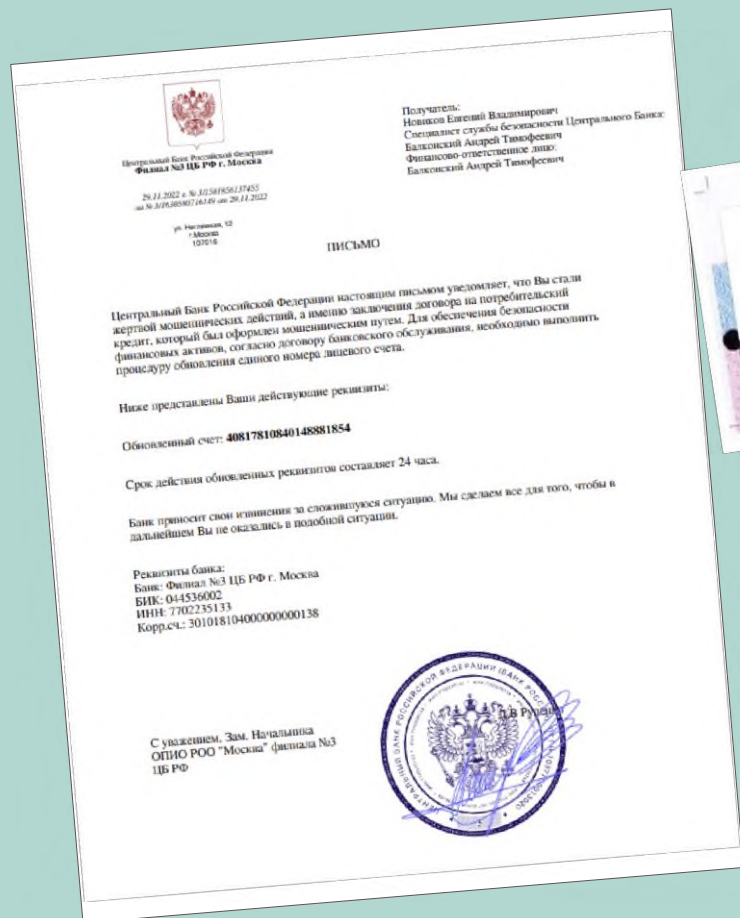
отрицательные

- страх
- паника
- чувство стыда

«С вашего счета списали все деньги»
«Ваш родственник попал в аварию
и сбил человека»
«Вас беспокоит следователь
Следственного комитета, вы участник
уголовного дела»



ЛЖЕСОТРУДНИКИ ЦЕНТРОБАНКА: ФАЛЬШИВЫЕ ДОКУМЕНТЫ

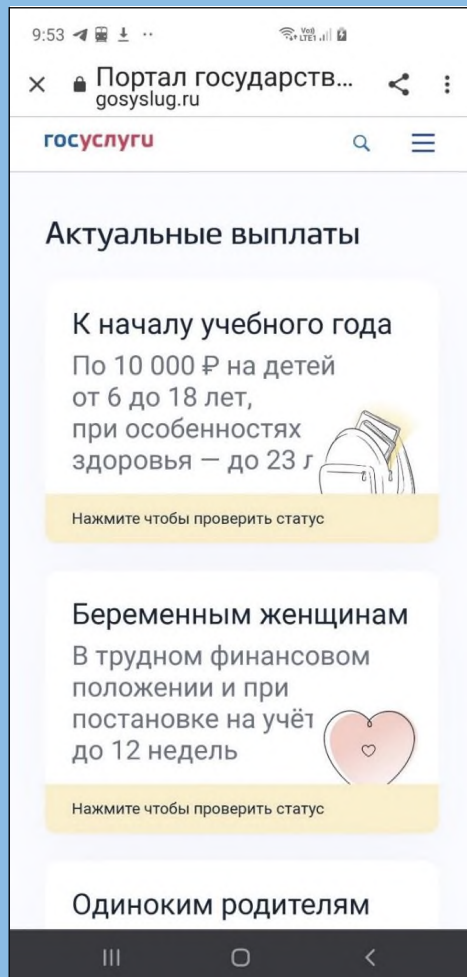




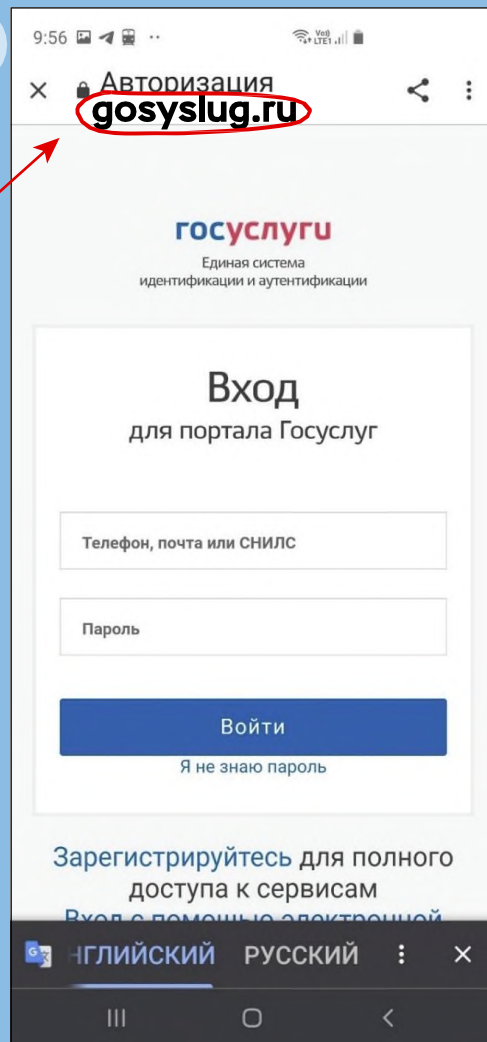
Банк России

САЙТЫ, МАСКИРУЮЩИЕСЯ ПОД «ГОСУСЛУГИ»

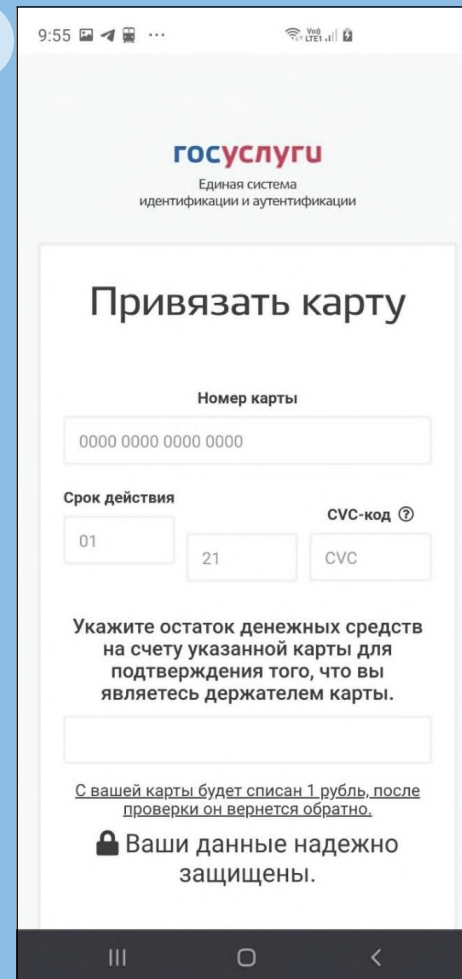
1



2



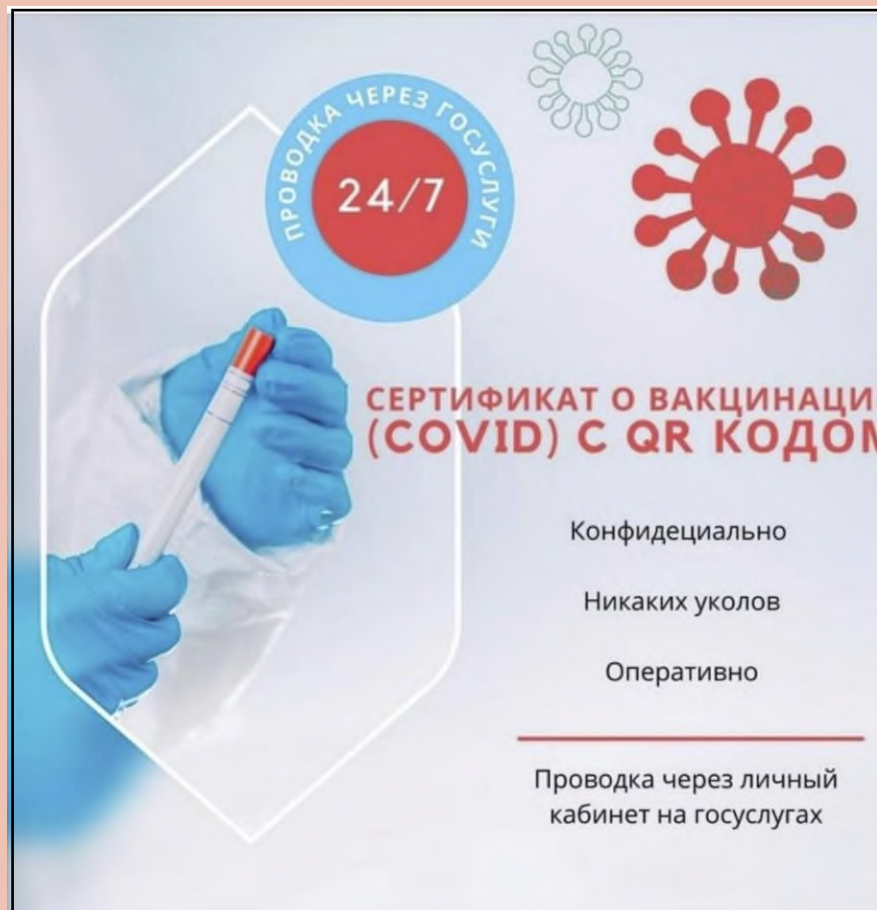
3





Банк России

НОВОСТНОЙ ФИШИНГ



ПРОВодКА ЧЕРЕЗ ГОСУСЛУГИ
24/7

СЕРТИФИКАТ О ВАКЦИНАЦИИ
(COVID) С QR КОДОМ

Конфиденциально

Никаких уколов

Оперативно

Проводка через личный кабинет на госуслугах



Мы находим
непризывные
заболевания у 90%
парней, скорее всего
ты в их числе

При грамотном подходе можно найти заболевание почти у каждого юноши. Даже если ты считаешь себя полностью здоровым, при скрупулезном обследовании в клиниках Воеводы у тебя можно найти болячки, освобождающие от армии. Благодаря кам клиенты вовремя обнаруживали у себя опасные диагнозы (например, киста головного мозга). Поэтому нельзя быть уверенным в своем здоровье на сто процентов.

ОФОРМИТЬ





ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ

- ✓ **Не сообщайте никому личную и финансовую информацию (данные карты)**
- ✓ **Установите антивирусные программы на все свои гаджеты и регулярно обновляйте их**
- ✓ **Не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам**
- ✓ **Не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы**
- ✓ **Заведите отдельную банковскую карту для покупок в Интернете**



**Будьте бдительны:
не действуйте второпях и проверяйте информацию!**

Расскажите эти правила поведения своим друзьям и знакомым!



Банк России

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ



Самостоятельно звоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка



Установите двухфакторный способ аутентификации – например, логин и пароль + подтверждающий код из СМС



Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой



**Будьте бдительны:
не действуйте впопых и проверяйте информацию!**

Расскажите эти правила поведения своим друзьям и знакомым!



Банк России

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

1

Не отвечайте
на звонки с незнакомых
номеров

2

Прервите разговор,
если он касается
финансовых вопросов

3

Не торопитесь
принимать решение

4

Проверьте информацию
в Интернете
или обратитесь за помощью
к близким родственникам



5

Самостоятельно
позвоните
близкому человеку /
в банк / в организацию

6

Не перезванивайте
по незнакомым
номерам



Возьмите паузу
и спросите совета
у родных и друзей!