

Памятки и правила поведения при угрозе кибермошенничества

Будь умней телефонных
мошенников!

Клади
трубку



Без разговоров





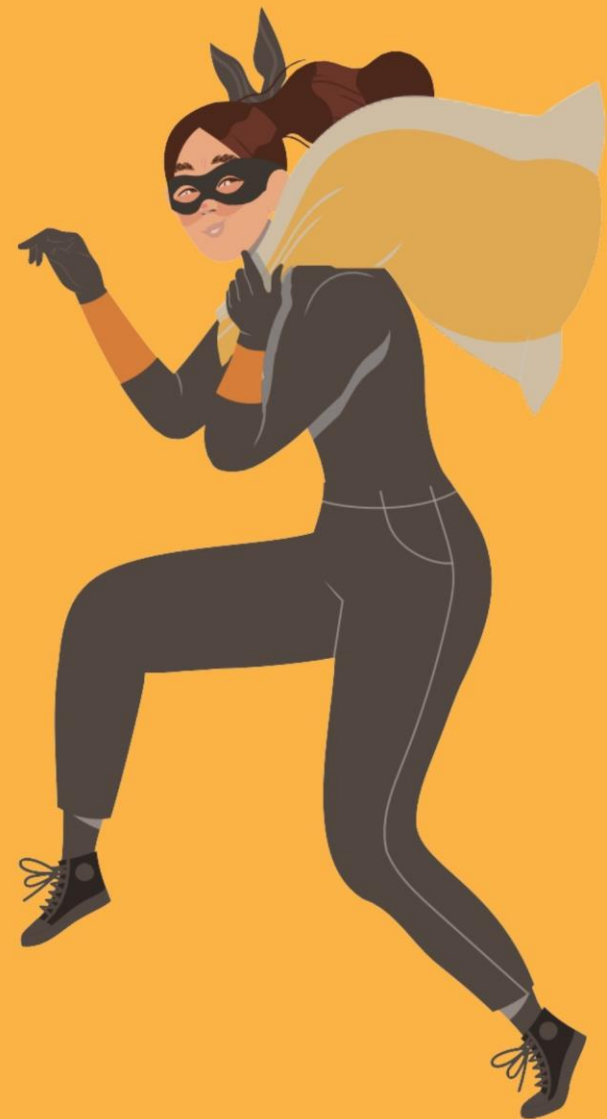
Банк России

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

«По вашей карте зафиксирована сомнительная операция.

«ЛЖЕСОТРУДНИК (БАНКАЦЕНТРОБАНКА РОССИИ)» Для сохранности денег вам нужно перевести их на «безопасный» («специальный») счет в Центробанке»

«ПРЕДСТАВИТЕЛЬ
ПРАВООХРАНИТЕЛЬНЫ
Х

«Следователь Следственного комитета.

ОРГАНОВ
(МВД, ФСБ, СК РФ)»

«Следователь Следственного комитета.

Вы являетесь свидетелем по уголовному делу № 123/2024 в отношении Иванова В.В., капитана
Иванов В.В., капитана ИЦива. По вашему поручению оформлен кредит
подтверждение оформления кредита указав на карту. Необходимо уточнить
нам необходимые 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»



Банк России

ЛЖЕСОТРУДНИКИ ЦЕНТРОБАНКА: ФАЛЬШИВЫЕ ДОКУМЕНТЫ

Получатель:
Никишов Евгений Владимирович
Специалист службы безопасности Центрального Банка
Балковский Андрей Тимофеевич
Финансово-ответственное лицо
Балковский Андрей Тимофеевич

ПИСЬМО

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы стали жертвой мошеннических действий, а именно заключения договора на потребительский кредит, который был оформлен мошенническим путем. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого номера лицевого счета.

Ниже представлены Ваши действующие реквизиты:

Обновленный счет: **40817810840148881854**

Срок действия обновления реквизитов составляет 24 часа.

Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: Филиал №3 ЦБ РФ г. Москва
БИК: 044536002
ИНН: 7702351133
Корр.сч.: 301018104000000000138

С уважением, Зам. Начальника
ОГИБО РОО "Москва" филиала №3
ЦБ РФ



Получатель:
Никишов Евгений Владимирович
Специалист службы безопасности Центрального Банка
Балковский Андрей Тимофеевич
Финансово-ответственное лицо
Балковский Андрей Тимофеевич

ПИСЬМО

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, единого лицевого счета, необходимо выполнить процедуру обновления.

Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Удаление лицевого счета из системы ЦБ РФ. Процедура выполняется, если сумма всех финансовых активов составляет менее 100 000,00 рублей. В случае, если баланс по результатам мошеннических действий превышает страховочную сумму, которая была погашена в пользу Банка (сумма ФЭЗ "О" противостоит сумме выданных средств из резервного фонда), в финансовом управлении территориального управления Банка, получившем контроль.

II этап:
- Активация обновленного счета. Выполняется методом внесения финансовых активов, предоставленных вам с резервного фонда ЦБ РФ. Внесение выполняется записывающим представителем технического отдела.

Уведомление Вас:
- о нарушении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (См. статью 183 УК РФ (обладание похищенной информацией, коммерческой, налоговой и банковской тайны)).
- о финансовых вложениях (за отток) или нарушении выполнения регламента - исполнение кредитной организации (сумма ст. 81 УПК РФ) и вложения денежных средств, выделенных Банком для выполнения регламентных действий (поиск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

* Пропущенная ставка по банковскому вкладу после обновления реквизитов понижается на 1,5% годовых.

Срок обновления реквизитов с момента выполнения работ, составляет 24 часа.

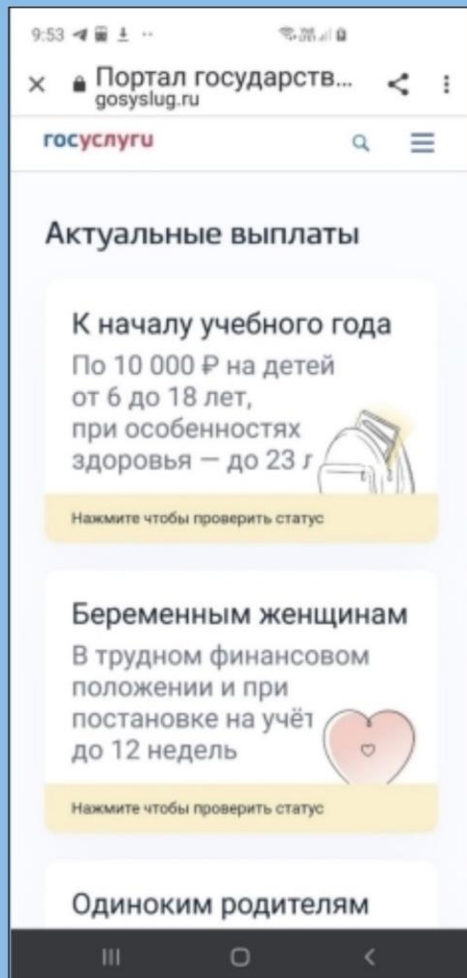
С уважением, Зам. Начальника
ОГИБО РОО "Москва" филиала №3
ЦБ РФ



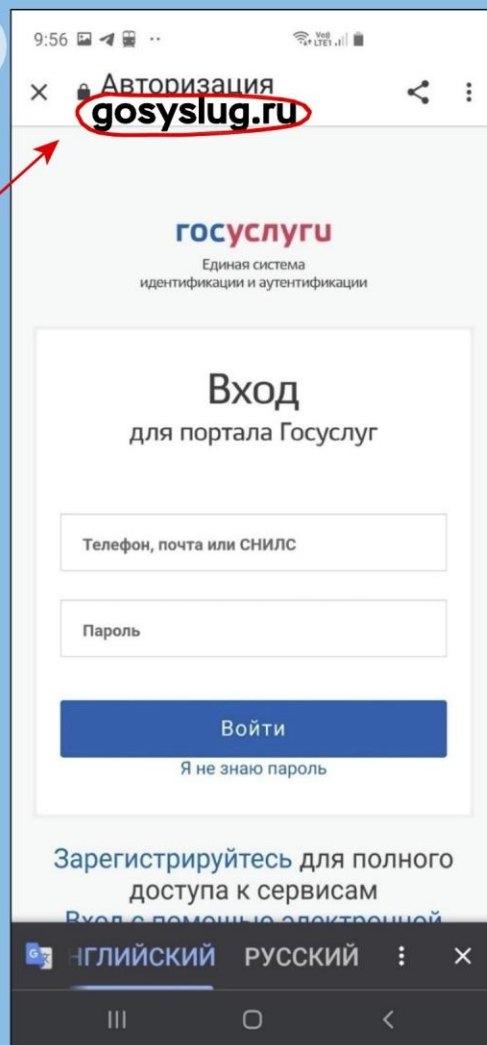
Банк России

САЙТЫ, МАСКИРУЮЩИЕСЯ ПОД «ГОСУСЛУГИ»

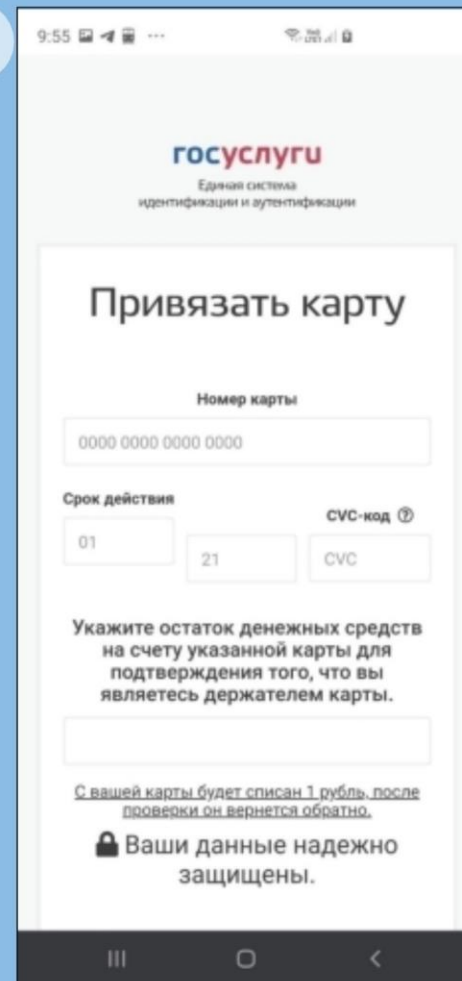
1



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 Вологды у тебя можно найти болячки, освобождающие от армии. Благодаря нам 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 впопыхах и проверяйте информацию!**

Расскажите эти правила поведения своим друзьям и знакомым!



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!

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 СМСсообщения.

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, онлайнбанк) 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 оборотной 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 чреватые 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!

Приложение 5 к письму Южного
ГУ Банка России «Об участии в ИК
«Клады трубку»

Ссылка на материалы:

Макеты печатных материалов (листовки, плакаты)	
https://disk.yandex.ru/d/qzvSpMKH3A_XOQ	
Видео ролики	
https://disk.yandex.ru/d/jTnTYe9KyCXWow	
Аудио ролики	
https://disk.yandex.ru/d/GhH3I9I2yATzsQ	
Заставки для рабочих столов	
https://disk.yandex.ru/d/5CVR348kKH1Rjg	
Социальные сети (карточки, баннеры)	
https://disk.yandex.ru/d/Jg6WU88TLsz3yg	