СБЕРБАНК

Всегда рядом

Памятка по кибербезопасности

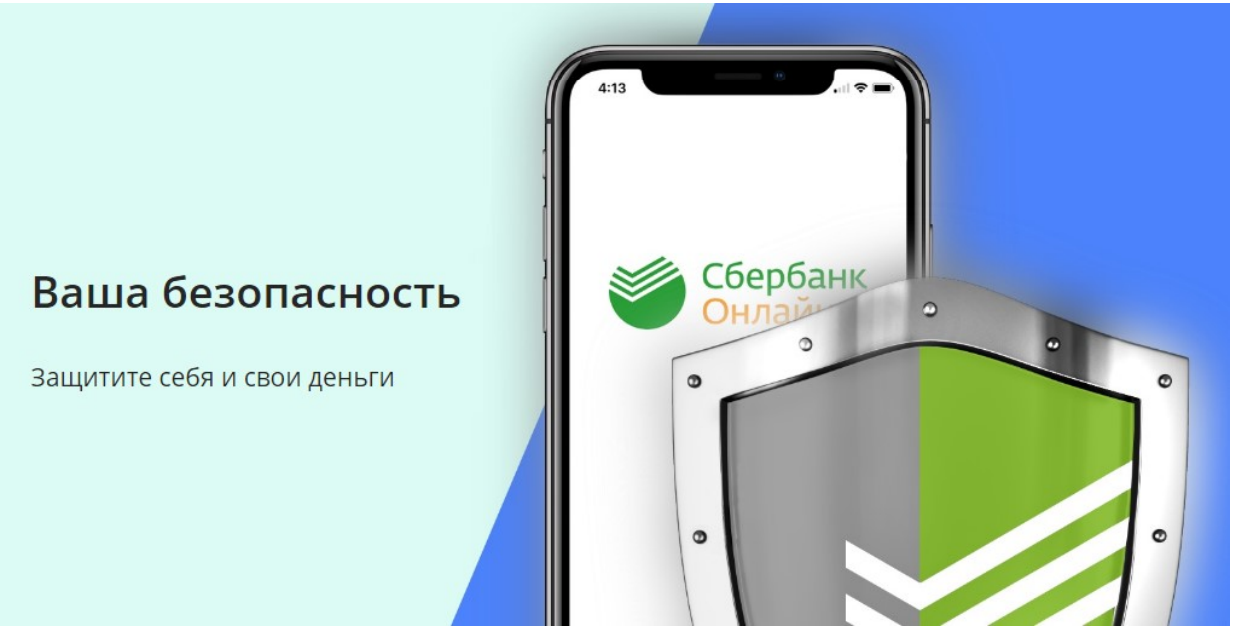
Саратов, 2020 г.

СБЕРБАНК

1

Рекомендации по безопасности

- ✓ Наша главная задача — сохранность ваших денег и личных данных
- ✓ Мы постоянно блокируем новые угрозы и используем самые современные средства защиты
- ✓ **Но самая надёжная защита — это ваша осведомленность, бдительность и осторожность!**



СБЕРБАНК

2

Способы обратной связи

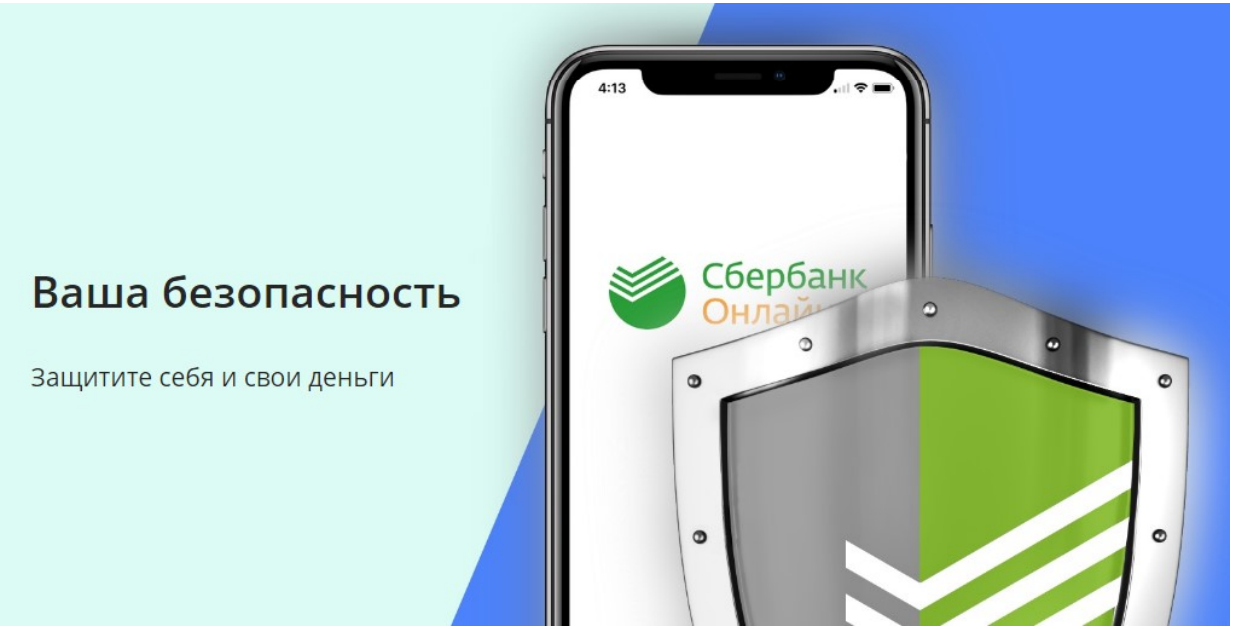
Мы всегда на связи

Столкнулись с мошенниками? Срочно звоните:

В мобильном приложении
Нажмите иконку телефона в левом верхнем углу

На номер 900
С мобильного телефона, звонки по России бесплатные

На номер +7 495 500-55-50
для звонков из любой точки мира, по тарифам оператора



СБЕРБАНК

3

Сообщение о мошенничестве

Давайте бороться с мошенниками вместе

Вы столкнулись с чем-то подозрительным — например, обнаружили поддельный сайт или аккаунт в соцсетях с логотипом Сбербанка?
Или стали свидетелем действий мошенников — например, они под видом сотрудников позвонили вашим родственникам?

Напишите нам, мы примем меры.

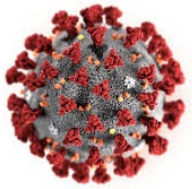
https://www.sberbank.ru/ru/person/dist_services/warning/form

4

Мошенники и коронавирус

Осторожно: мошенники используют тему коронавируса как приманку

- Если видите в почте письмо со словом «коронавирус» в теме, будьте осторожны и не переходите по ссылкам — там может оказаться сайт-ловушка.
- Внимательно проверяйте ссылки в письме, особенно короткие. Не оставляйте свои данные на подозрительных сайтах.
- Доверяйте только официальным аккаунтам Сбербанка в соцсетях и не сообщайте никому пароли из СМС и номера карты — мошенники часто пишут от имени Сбербанка.



СБЕРБАНК

5

Правила личной кибербезопасности

Правила личной кибербезопасности

Эти простые правила должен знать каждый, кто не хочет быть обманутым и лишиться денег

Узнайте о распространённых приёмах злоумышленников и не дайте им себя обмануть

СБЕРБАНК

6

Правила личной кибербезопасности

Главные правила личной кибербезопасности

Не сообщайте никому свои пароли, ПИН- и CVV-коды и **коды из СМС.** Даже сотрудникам банка

Не переходите по подозрительным ссылкам: мошенники могут заразить ваш компьютер или телефон вирусом и украсть ваши данные

Используйте только официальные приложения банка в App Store, Google Play и Microsoft Store

Используйте антивирусы. Приложение Сбербанк Онлайн на Android имеет бесплатный антивирус

Сообщите банку о смене номера мобильного: есть риск, что ваши данные попадут новому владельцу

Проверяйте реквизиты переводов и платежей, которые приходят в СМС от банка

СБЕРБАНК

7

Правила личной кибербезопасности

Официальные номера Сбербанка

Сбербанк отправляет СМС только с номеров 900 и 9000

С номера 9000 банк проводит СМС-опрос о качестве обслуживания и проводит актуализацию данных.

Сообщение может содержать ссылку на портал Центра недвижимости Сбербанка Domclick.ru или опрос Сбербанка.

При использовании банкоматов

- **Прикрывайте клавиатуру рукой**, когда вводите ПИН-код
- **Не принимайте помощь от незнакомцев, находясь у банкомата,** и не совершайте операции под диктовку
- **Осмотрите банкомат перед использованием** и убедитесь, что на нём нет подозрительных устройств

СБЕРБАНК

8

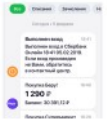
Правила личной кибербезопасности

Пользуйтесь услугами банка безопасно

Что нужно знать при использовании финансовых сервисов

Интернет-банк

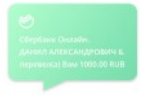
Мобильное приложение



Сервис СМС-банк

Банкоматы

Банковская карта



СМС- и email-мошенничество

Телефонные мошенники

Псевдоброкеры и псевдодилеры

СБЕРБАНК

9

Правила пользования интернет-банком

Как безопасно пользоваться интернет-банком

Интернет-банк Сбербанк Онлайн — удобный и безопасный способ совершать банковские операции на компьютере, без визита в банк. Чтобы защитить себя от мошенников, достаточно соблюдать простые правила:

Никому не сообщайте пароли для входа в Сбербанк Онлайн
Даже своим близким и сотрудникам банка.

Убедитесь, что адресная строка начинается с префикса https://
Это означает, что установлено защищенное соединение

Никогда не вводите пароли для отмены операции
Об этом могут попросить только мошенники. Если вы с этим столкнулись, покиньте сайт и срочно обратитесь в банк

Старайтесь не пользоваться веб-версией Сбербанк Онлайн с мобильного телефона
Намного удобнее использовать мобильное приложение

10

Правила пользования интернет-банком

СБЕРБАНК

Как безопасно пользоваться интернет-банком

Интернет-банк Сбербанк Онлайн — удобный и безопасный способ совершать банковские операции на компьютере, без визита в банк. Чтобы защитить себя от мошенников, достаточно соблюдать простые правила:

Используйте только официальный сайт Сбербанк Онлайн
Сохраните этот адрес в закладках браузера (посмотреть примеры сайтов-подделок можно ниже)

Проверяйте реквизиты операции в СМС с одноразовым паролем от номера 900
Если реквизиты не совпадают, то такой пароль вводить нельзя

Используйте антивирус
Регулярно делайте полную проверку компьютера программой-антивирусом. Установите автоматическое обновление антивирусных баз и операционной системы

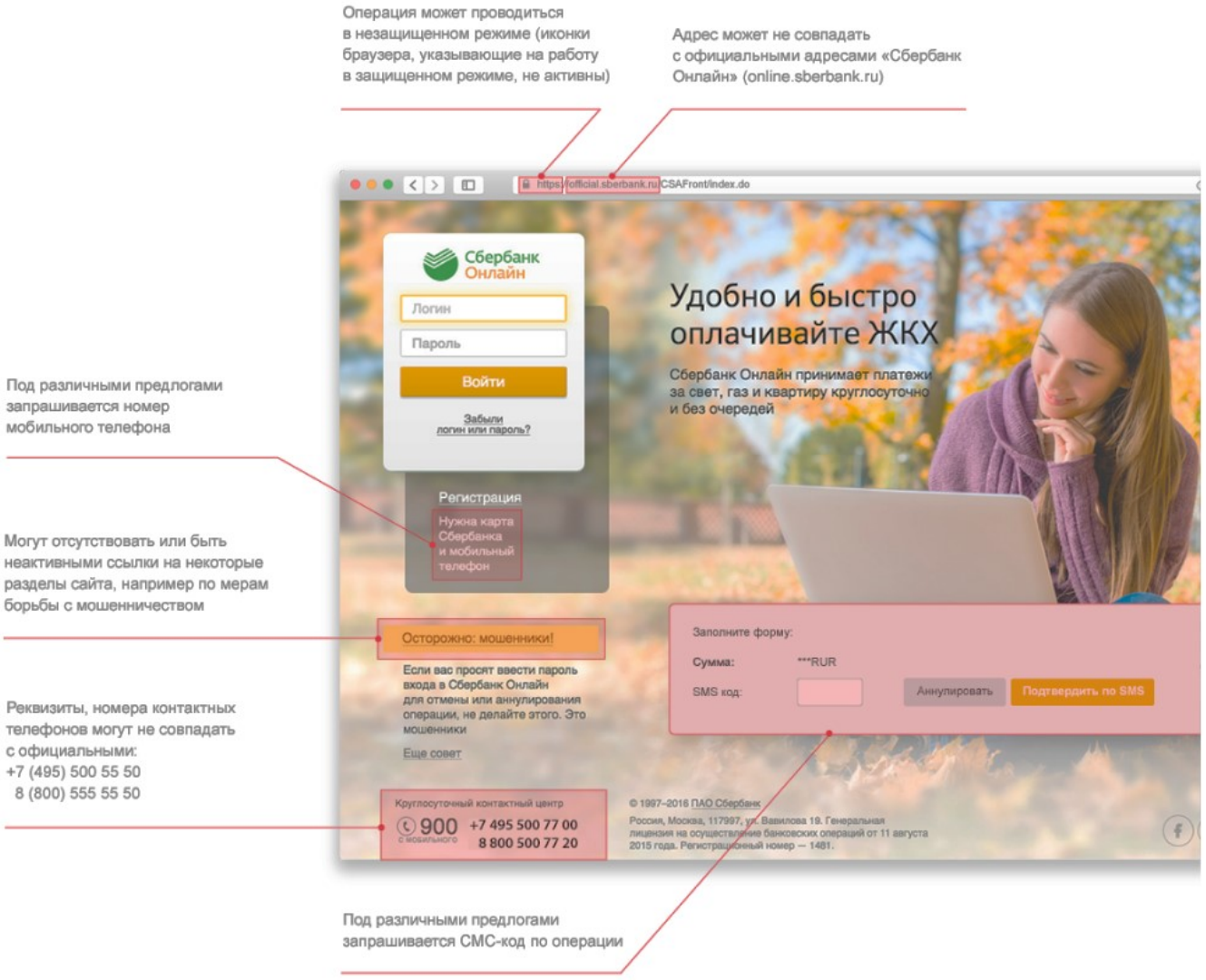
Для входа в Сбербанк Онлайн нужен только логин, личный пароль или одноразовый из СМС
Если на сайте запрашивают любую другую персональную информацию, например, номер банковской карты или мобильного телефона, покиньте сайт и срочно обратитесь в банк

СБЕРБАНК

11

Правила пользования интернет-банком

Как распознать сайт-«подделку»?

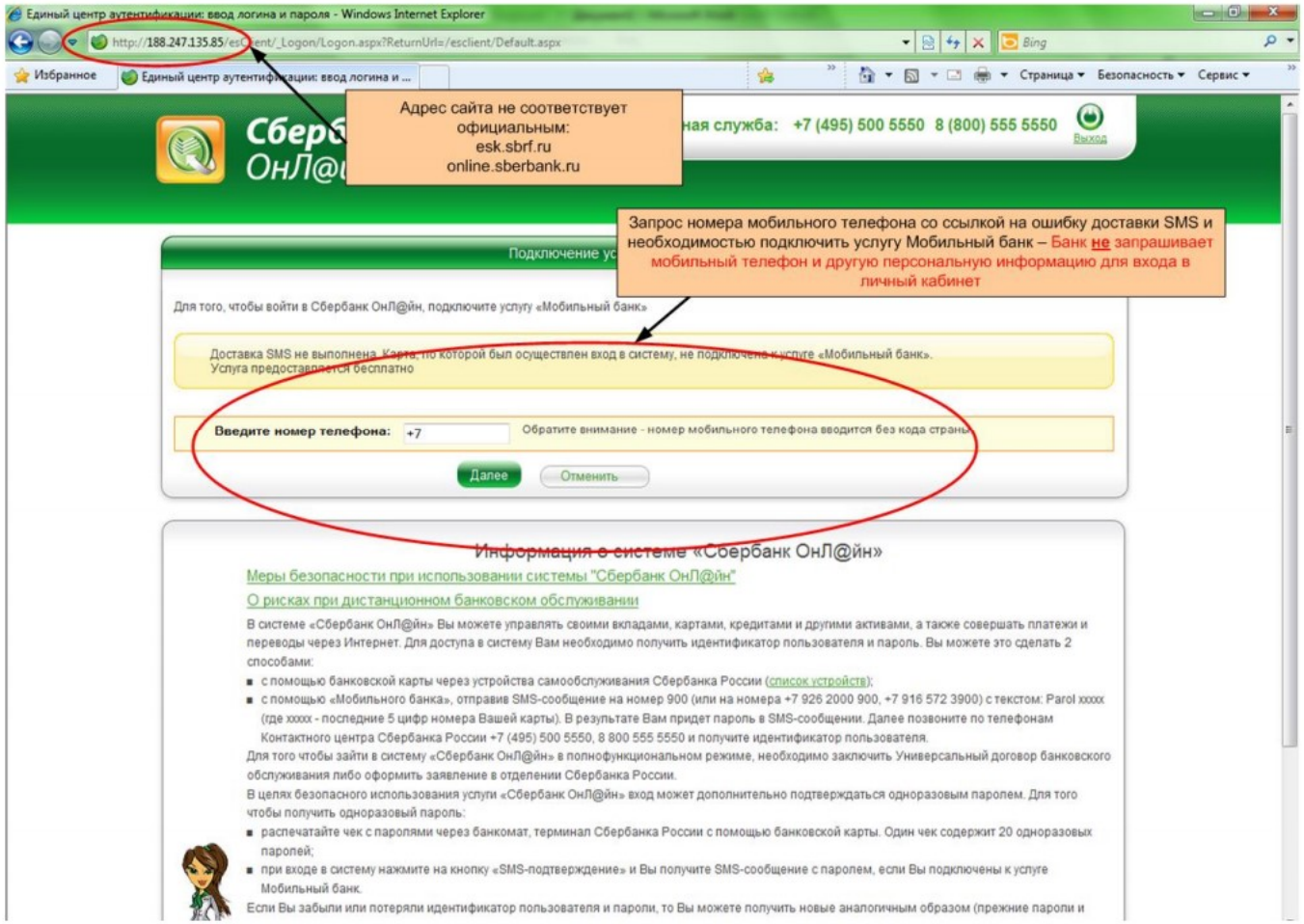


СБЕРБАНК

12

Правила пользования интернет-банком

Примеры фишинговых сайтов

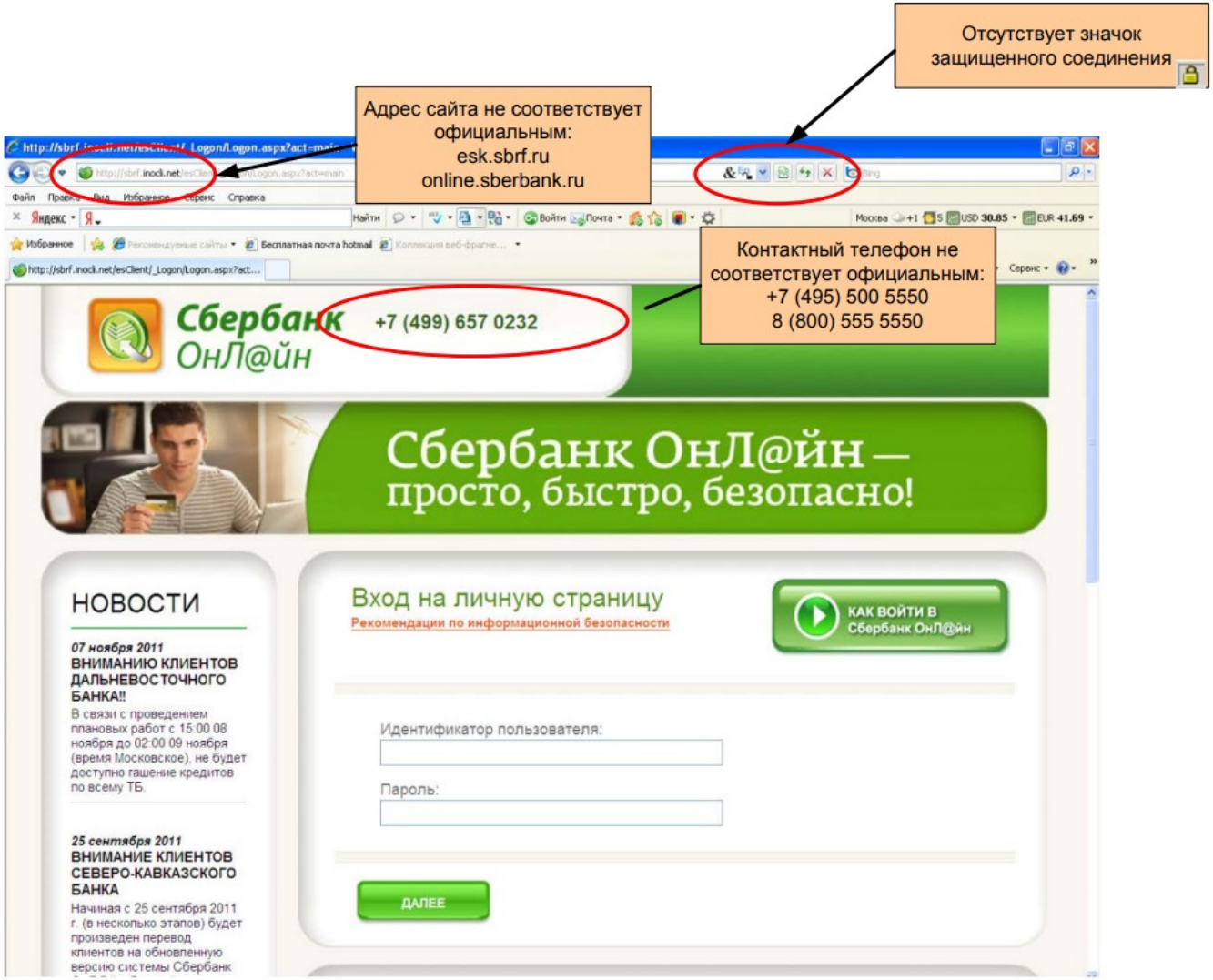


СБЕРБАНК

13

Правила пользования интернет-банком

Примеры фишинговых сайтов

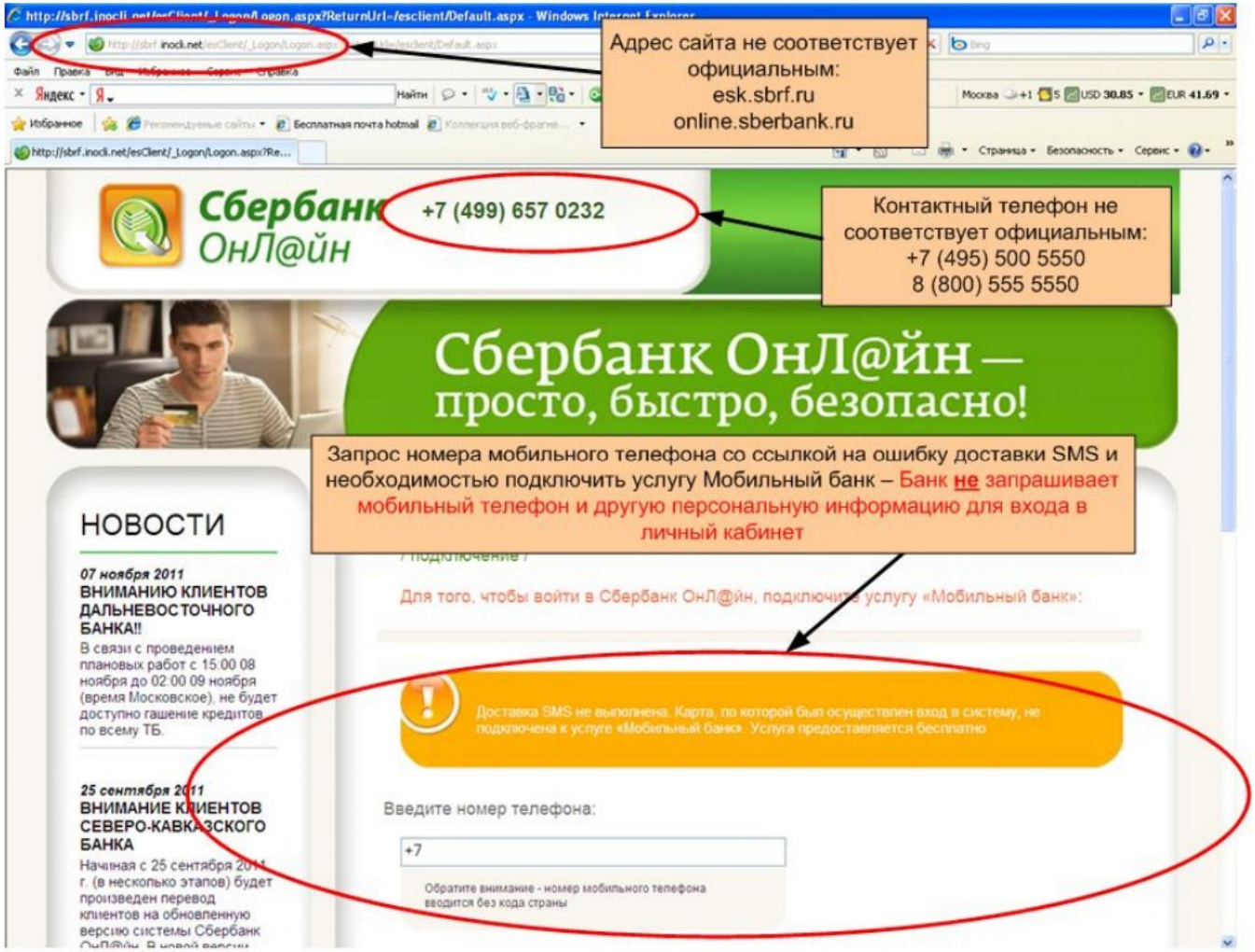


СБЕРБАНК

14

Правила пользования интернет-банком

Примеры фишинговых сайтов

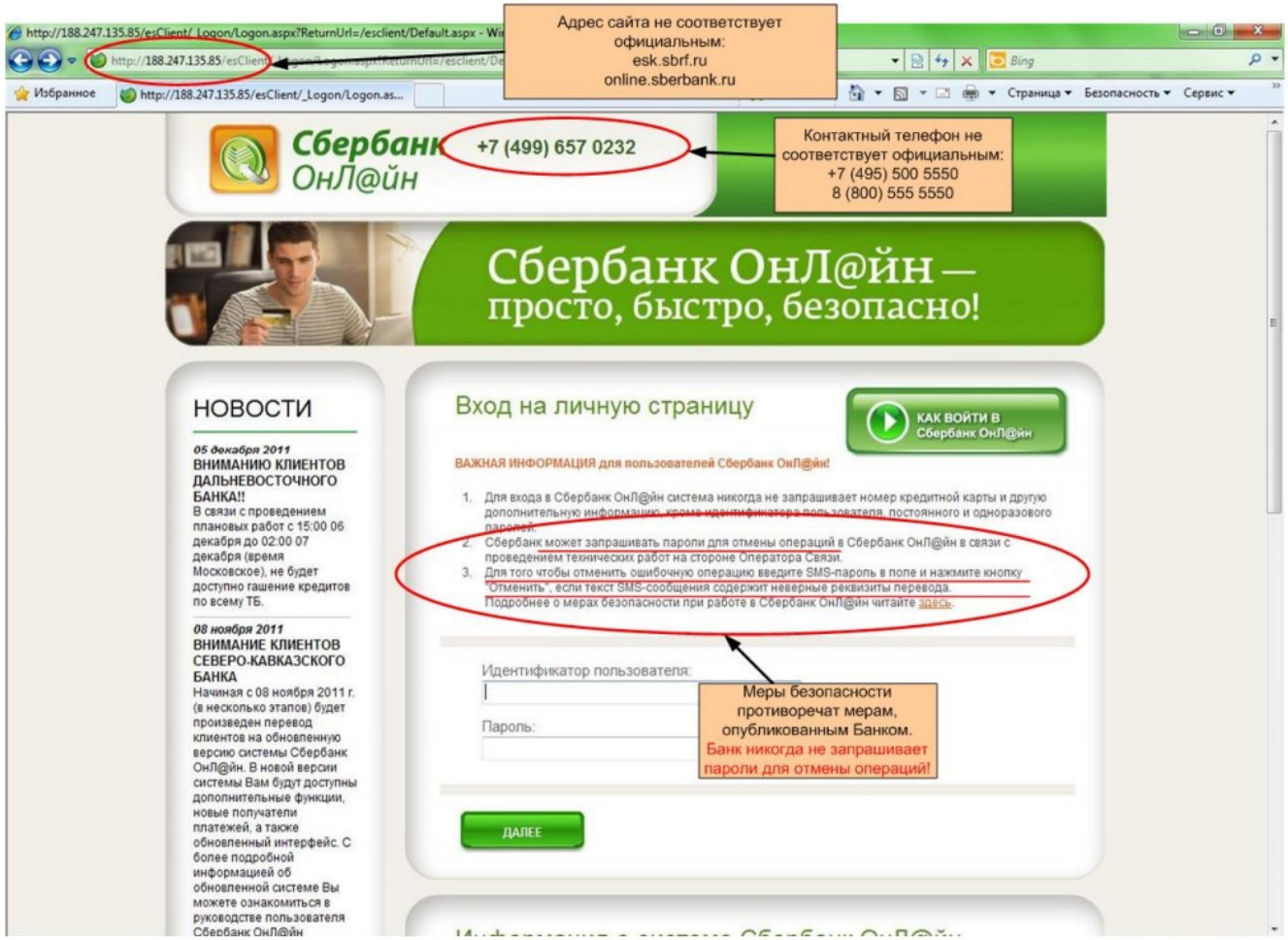


СБЕРБАНК

15

Правила пользования интернет-банком

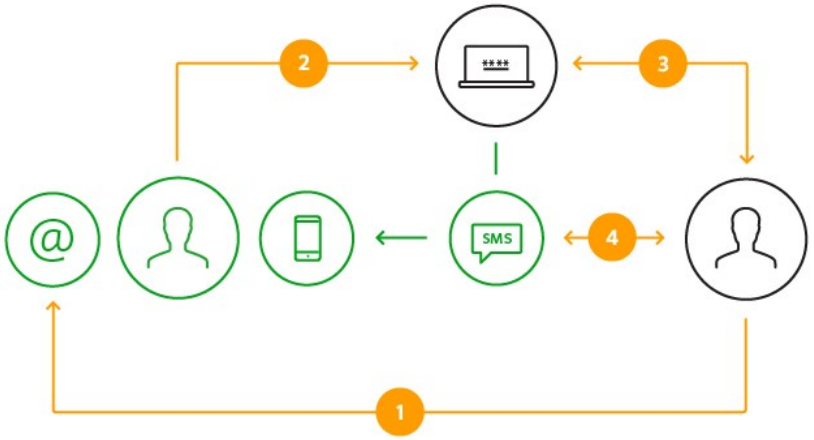
Примеры фишинговых сайтов



16

Правила пользования интернет-банком

Как мошенники крадут деньги с помощью фишинга. Схема 1



Классическая схема мошенничества

1

Фишинговый сайт

Злоумышленник на различных ресурсах от социальных сетей и электронной почты до обычных новостных сайтов — заставляет Вас нажать на ссылку, ведущую на фишинговый сайт. Вы переходите на поддельный сайт, который копирует дизайн и содержание известного сайта.

2

Персональные данные

На поддельном сайте Вас могут попросить ввести идентификаторы и пароли, мобильный телефон и другие персональные данные, необходимые мошенникам для обмана. Для защиты от мошенников в «Сбербанк Онлайн» предусмотрено подтверждение финансовых операций одноразовым паролем, который отправляется вместе с реквизитами самой операции. Необходимость подтверждения операции одноразовым паролем отображается в «Сбербанк Онлайн» при совершении операции.

3

Одноразовый SMS-пароль

Злоумышленнику нужно узнать у Вас одноразовый SMS-пароль для проведения операции, Как правило, мошенник звонит Вам на телефон и представляется сотрудником банка и просьбами или угрозами заставляет продиктовать ему Ваш одноразовый пароль.

4

Не разглашайте никому одноразовый пароль

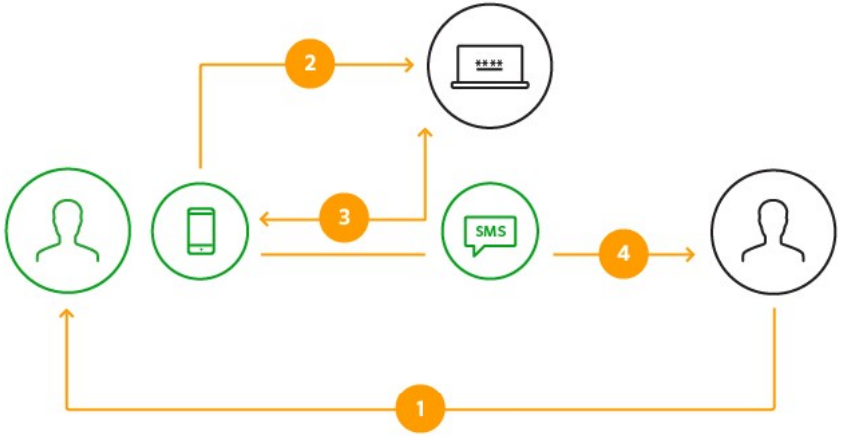
Поэтому одноразовый пароль это очень критичный элемент безопасности — его нельзя никому разглашать и ни в коем случае нельзя вводить, если полученные в SMS-сообщении реквизиты относятся к операции, которую Вы не совершали.

СБЕРБАНК

17

Правила пользования интернет-банком

Как мошенники крадут деньги с помощью фишинга. Схема 2



Для мобильных устройств

1

Вирус

Вирусное программное обеспечение (вирус) заражает мобильное устройство клиента.

2

Сайт — ловушка

При попытке клиента открыть с мобильного устройства сайт банка, вирус перенаправляет клиента на специальный сайт-ловушку, имитирующий сайт Сбербанка.

3

На поддельном сайте

На поддельном сайте могут предложить ввести логин и пароль от личного кабинета, пройти социальный опрос, скачать антивирус или новое приложение от Сбербанка.

4

Вирус самостоятельно получает и пересылает SMS-пароли

После установки вирус самостоятельно от имени клиента получает и пересылает злоумышленникам SMS-пароли для входа и подтверждения мошеннических операций в Сбербанк Онлайн.

СБЕРБАНК

18

Правила пользования мобильным приложением

Как безопасно пользоваться мобильным приложением

Мобильное приложение Сбербанк Онлайн — удобный и безопасный способ управлять своими финансами на смартфоне. Мы делаем всё, чтобы пользоваться им было безопасно: например, в наше приложение на платформе Android уже встроен антивирус. Тем не менее, просим вас соблюдать простые правила:

Никому не говорите пароль для входа в мобильное приложение

Используйте только официальные приложения банка для Android, iPhone, iPad и Windows Phone

При установке на смартфон любых приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к интернету — оно может быть опасным, лучше не устанавливайте его.

Не устанавливайте приложения по ссылкам из СМС-сообщений или электронной почты, даже если в сообщении утверждается, что оно из банка.

Отключите в настройках вашего iPhone возможность использовать голосовое управление Siri при заблокированном экране (Настройки — Siri — Доступ с блокировкой экрана).

Не модифицируйте операционную систему телефона (например, с помощью джейлбрейка). Несанкционированная модификация отключает защитные механизмы, заложенные производителем, и ваш телефон становится уязвимым к заражению вирусными программами.

СБЕРБАНК

19

Правила пользования сервисом СМС-банк

Как безопасно пользоваться сервисом СМС-банк

Сервис СМС-банк — это способ получать банковские услуги с помощью СМС-сообщений через номер 900, USSD-запросов, а также Push-уведомлений (при наличии Мобильного приложения Сбербанк Онлайн). Сервис даёт возможность отправлять банку СМС-поручения на номер 900 — например, команды на совершение перевода и многое другое. Чтобы пользоваться сервисом без опасений, соблюдайте простые правила:

Установите сложный пароль на телефоне
Иначе мошенникам будет проще добраться до ваших денег

Если потеряли телефон, обратитесь в банк
И попросите временно заблокировать СМС-банк. Затем заблокируйте свою сим-карту у сотового оператора.

Если вдруг перестала работать сим-карта, позвоните своему оператору связи и выясните причину
Возможно, вас атакуют мошенники

Если вы сменили номер мобильного телефона
Отключить СМС-банк Вы сможете в Мобильном приложении «Сбербанк Онлайн» или Банкомате.

Не подключайте к СМС-банку чужие телефоны
Даже если вас просят об этом люди, которые представились «сотрудниками банка».

Отключите в настройках iPhone голосовое управление Siri при заблокированном экране
Как отключить: Настройки → Siri → Siri с блокировкой экрана

Когда банк видит подозрительные операции от вашего имени, он может по своей инициативе временно заблокировать доступ к сервисам СМС-банк и Сбербанк Онлайн. Если операции совершали вы, для быстрого возобновления доступа позвоните, пожалуйста, в контактный центр Сбербанка по номеру 900 (с мобильного телефона, звонок на территории России бесплатный).

СБЕРБАНК

20

Правила пользования банкоматами

Как безопасно пользоваться банкоматами

При использовании банкоматов помните о простых правилах безопасности:

При наборе ПИН-кода прикрывайте клавиатуру рукой. Если вокруг нет людей — это еще не означает, что мошенники за вами не наблюдают.

Отдавайте предпочтение банкоматам, установленным в защищенных местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

Если на входе в помещение с банкоматом установлено устройство, которое требует ПИН-код вашей карты, не вводите ПИН и не входите туда.

Не используйте банкомат в присутствии подозрительных лиц. Подождите, пока они разойдутся, или воспользуйтесь другим банкоматом

Не принимайте помощь от незнакомцев. Находясь у банкомата, не прислушивайтесь к советам незнакомых людей и не принимайте их помощь. Если вам нужна помощь, обратитесь к сотруднику банка или позвоните в контактный центр банка по номеру 900 (звонок с мобильного телефона на территории России бесплатный).

Осмотрите банкомат перед использованием. Убедитесь, что на клавиатуре и в месте для приема карт нет дополнительных устройств. Обращайте внимание на неисправности и повреждения — например, на неровно установленную клавиатуру. Если что-то вызвало подозрения, не пользуйтесь этим банкоматом.

Перед использованием банкомата убедитесь, что все операции, совершаемые предыдущим клиентом, завершены. Если у вас возникают сомнения, нажмите кнопку «Отмена».

Не используйте неисправный банкомат. Если банкомат зависает, самопроизвольно перезагружается или на экране появляются подозрительные изображения — не пользуйтесь им. Отмените текущую операцию, нажав кнопку «Отмена», и дождитесь возврата карты.

Если банкомат не возвращает карту, позвоните на номер 900 или по телефону, указанному на банкомате. Не отходите от банкомата, пока не выполните рекомендации сотрудника банка.

СБЕРБАНК

21

Правила пользования банковской картой

Как безопасно пользоваться банковской картой

Банковская карта — ключ доступа к вашему счету. Относитесь к ней так же бережно, как к наличным. Чтобы обезопасить себя от мошенников, следуйте простым рекомендациям:

Никому не передавайте карту

Никому не говорите и не записывайте свой ПИН-код

Храните карту в месте, недоступном для посторонних

Не вводите ПИН-код нигде в интернете

Как обезопасить свою карту

Не оставляйте карту без присмотра и не передавайте никому — ни официантам, ни коллегам, ни родственникам. Детям можно оформить дополнительную карту к родительской, а взрослые могут открыть свою собственную карту.

Если вы потеряли карту или подозреваете, что ваш счёт атакуют мошенники, срочно её заблокируйте. Для этого позвоните в контактный центр Сбербанка на номер 900 с мобильного телефона (звонок в России бесплатный). Или зайдите в интернет-банк или мобильное приложение Сбербанк Онлайн — найдите нужную карту и нажмите «Заблокировать».

Не совершайте покупки с общедоступных компьютеров или с использованием бесплатного Wi-Fi — мошенники могут украсть данные вашей карты.

Выбирайте для покупок только те интернет-магазины, в которых вы точно уверены.

Не соглашайтесь на предложения купить вашу карту — её могут использовать в мошеннических целях. Правоохранительные органы в первую очередь будут проверять владельца карты на причастность к преступлению.

СБЕРБАНК

22

Правила пользования банковской картой

Как безопасно пользоваться банковской картой

Банковская карта — ключ доступа к вашему счету. Относитесь к ней так же бережно, как к наличным. Чтобы обезопасить себя от мошенников, следуйте простым рекомендациям:

Как обезопасить ПИН-код

Не записывайте ПИН-код на бумаге, на самой банковской карте, в телефоне или компьютере — просто запомните его.

Периодически меняйте ПИН-код — примерно раз в 3 месяца. Для этого в банкомате или устройстве самообслуживания Сбербанка зайдите в раздел «Личный кабинет, информация и сервис» и выберите пункт «Сменить ПИН-код».

Никому не сообщайте ПИН-код. Даже родственникам и сотрудникам банка.

Как контролировать операции по картам

Подключите Уведомления по карте – вам на телефон будут приходить оповещения о каждой операции. Если вы вовремя отследите покупку или перевод, которые вы не совершали, вернуть деньги будет легче.

Регулярно проверяйте выписки с банковских счетов и квитанции о покупках, чтобы убедиться, что с вашими операциями всё в порядке. Сообщайте в банк о любых несоответствиях.

Сохраняйте чеки после оплаты и картой, и наличными, если первоначально оплата по карте из-за сбоев не прошла.

СБЕРБАНК

23

СМС и email мошенничество

Как обезопасить себя от СМС и email мошенничества

Мошенники регулярно рассылают СМС и электронные письма, замаскированные под сообщения от банка. Их цель — получить доступ к вашему счёту и украсть деньги. Поэтому важно уметь отличать официальные сообщения банка от писем мошенников.

Важно знать

Сотрудники банка никогда не просят клиентов назвать конфиденциальные сведения (полный номер карты, PIN- и CVC-коды и т.п.) и не требуют совершать активные операции с картами

Сбербанк не отправляет сообщения с формой для ввода ваших персональных данных

Сбербанк не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные

Сбербанк не просит зайти в Сбербанк Онлайн по ссылке из письма

При любых сомнениях звоните в контактный центр Сбербанка на номер 900 (с мобильного телефона) или на номер, указанный на обратной стороне карты

СБЕРБАНК

24

SMS и email мошенничество

Примеры мошеннических писем и SMS

SMS «Ваша карта заблокирована»

Вы получили SMS примерно такого содержания: «Ваша карта заблокирована» или «По Вашей карте проведена операция на сумму N рублей». Текст содержит номер телефона и призыв срочно по нему позвонить. Когда вы перезваниваете, вам отвечает мошенник, который представляется вам сотрудником банка — например, службы безопасности или технической поддержки. Вас просят предоставить информацию или срочно совершить какие-то действия — например, разблокировать карту или отменить операцию.

Мошенники попытаются под различными предлогами получить у вас конфиденциальные данные: полный номер карты, ПИН-код, CVV, CVC-код, срок действия, или попросят подойти к банкомату или терминалу и ввести код — будто бы для разблокировки карты или отмены платежа. Эти данные мошенники используют для кражи денег, покупок и переводов с вашего счёта.

25

СМС и email мошенничество

Примеры мошеннических писем и СМС

Электронное письмо от имени Сбербанка

Вам приходит электронное письмо якобы от Сбербанка, замаскированное под официальное письмо. Мошенники требуют от вас быстрых действий или немедленного ответа. Часто отправители таких писем хотят напугать вас («Сообщение об увеличении задолженности», «Ваш счёт заблокирован») или сообщают о каком-то выигрыше. Письма могут содержать вложения, просьбу уточнить реквизиты карты, срочно позвонить по указанному в письме номеру телефона или перейти по ссылке. Адрес сайта обычно похож на официальные адреса сайтов Сбербанка. Будьте осторожными с такими письмами: не переходите по ссылкам и не открывайте вложения. Лучше перезвоните в контактный центр банка, чтобы проверить информацию.

26

SMC и email мошенничество

Примеры мошеннических писем и СМС

Сообщение со ссылками

Мошенники используют наше любопытство в своих целях. Вам может прийти СМС с интригующим содержанием: вам могут сообщать, что вы «выиграли суперприз» или поздравлять с праздниками. Такие сообщения часто содержат ссылки, по которой вам обещают дополнительную информацию о выигрыше или ссылку на скачивание поздравительной открытки. Делать этого не следует.

При переходе по этой ссылке на ваш телефон или компьютер может загрузиться приложение с вирусным программным обеспечением, или вы попадете на сайт-ловушку, на котором под различными предлогами мошенники попытаются получить персональные данные: идентификатор и пароль для входа в интернет-банк, кодовое слово, номера банковских карт, ПИН-коды, CVV и другую информацию.

СБЕРБАНК

27

Телефонное мошенничество

Как распознать мошенника по телефону?

Мошенники часто выдают себя за сотрудников банка. Например, вам на мобильный телефон звонит незнакомец, который представляется специалистом клиентской поддержки или службы безопасности и просит назвать реквизиты карты, подойти к банкомату и срочно выполнить несколько операций. Причина, с его слов, очень серьёзная: сбой в базе данных, угроза мошенничества или что-то подобное. Задача мошенника — напугать вас и не дать времени проанализировать ситуацию, поэтому он будет настаивать, чтобы вы выполнили его требования как можно быстрее.

Не теряйте бдительности и трезво оценивайте происходящее. При звонке клиенту сотрудник Сбербанка:

- всегда обращается по имени-отчеству;
- никогда не просит конфиденциальные сведения: полные реквизиты карты (номер карты, ПИН- и CVV-код), CVC-пароли банка;
- никогда не требует совершать операций с картой.

Для контакта с клиентами Сбербанк использует три номера:

900	8 800 555-55-50	+7 495 500-55-50

28

Псевдоброкеры и псевдодилеры

Как обезопасить себя от псевдоброкеров и псевдодилеров?

Мошенники регулярно предлагают клиентам брокерские или дилерские услуги, с помощью которых якобы можно преумножить свой капитал и осуществить высокодоходные инвестиции. При этом мошенники не имеют лицензий на осуществление такой деятельности и к реальным брокерам или дилерам не имеют никакого отношения. Их цель – вынудить клиента перевести им денежные средства.

Важно знать

- Прежде чем переводить деньги компании, убедитесь, что у нее есть лицензия на осуществление брокерской или дилерской деятельности.
- Если деньги переведены в компанию, зарегистрированную на территории другого государства, то споры придется решать в правовом поле иностранного государства, так как законы РФ на эти компании не распространяются.
- Если вы перевели деньги на счёт компании, банк не сможет их вернуть. Процедура chargeback, предусмотренная правилами платежных систем для возврата необоснованно списанных средств и рекламируемая мошенниками как механизм защиты инвесторов, в данном случае не применяется, т.к. списание со счетов происходит по инициативе самих клиентов, и услуга по переводу средств со счета карты на личный счет является оказанной. Кроме того, по действующему законодательству РФ банки не вмешиваются в договорные отношения между плательщиками и получателями средств, при этом законодательство РФ превалирует над правилами платежных систем.
- Перечень российских компаний, у которых есть соответствующая лицензия, представлен на сайте Центрального банка РФ в Справочнике участников финансового рынка.
- Ознакомиться с отзывами о компании и узнать о реальном опыте взаимодействия с ней можно на профильных сайтах/форумах.
- При любых сомнениях звоните в контактный центр Сбербанка на номер 900 (с мобильного телефона) или на номер, указанный на обратной стороне карты

29

Псевдоброкеры и псевдодилеры

Как обезопасить себя от псевдоброкеров и псевдодилеров?

Как клиенты попадаются на уловки мошенников

Клиенту звонят из компании, якобы предоставляющей брокерские или дилерские услуги. Ему обещают высокий доход, существенно выше, чем у конкурентов. Предложение кажется клиенту заманчивым, и он соглашается воспользоваться услугами этой компании и перевести деньги на карту третьего лица.

Будьте внимательны! Реальные брокерские или дилерские компании не просят перевести средства на карту третьего лица. Если вы выполните такой перевод, отозвать средства уже будет невозможно.

30

Псевдоброкеры и псевдодилеры

Как обезопасить себя от псевдоброкеров и псевдодилеров?

Чтобы вывести часть денег, нужно заплатить

Клиент зарегистрировался на сайте торговой площадки по бинарным опционам, пополнил свой баланс и получил уведомление о получении «бонусных доходов». Однако для вывода этих денег, необходимо «повысить свой торговый статус», т.е. внести дополнительную сумму. В итоге клиент вносит все больше и больше средств, но так и не получает возможности вывести свои деньги.

Помните! Из реальной брокерской или дилерской компании клиент всегда может вывести свои свободные денежные средства.

СБЕРБАНК

31

Псевдоброкеры и псевдодилеры

Как обезопасить себя от псевдоброкеров и псевдодилеров?

Осторожно, лотерея!

Клиент невнимательно читает договор, который подписывает с якобы брокерской компанией. Когда клиент пытается получить свои деньги, компания отказывает, ссылаясь на договор, где указано, что клиент участвовал в лотерее. Получается, что клиенту «просто не повезло» и он проиграл свои деньги.

Будьте бдительны! Всегда внимательно читайте договоры, которые вы подписываете. При любых сомнениях берите время на более детальное изучение документов.

СБЕРБАНК

32

Способы обмана

Как обманывают мошенники

Узнайте о распространённых приёмах злоумышленников и не дайте им себя обмануть

Ситуация 1. «Звонок из службы безопасности банка»

Вам звонит незнакомец

Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка».

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка, например, таких: +7900, +900

Злоумышленники могут поменять одну цифру в номере, которую вы не заметите и подумаете, что это банковский номер.

33

Способы обмана

Как обманывают мошенники

СБЕРБАНК

У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой».

Он просит у вас полные данные карты, CVV- или CCV-код, код из СМС или пароли от Сбербанк Онлайн. Это нужно якобы «для сохранности ваших денег».

Как мошенник может вас убеждать

- «Мы звоним с официального номера, проверьте на сайте».
- «В целях конфиденциальности я включаю программу-робот, которая защитит ваши конфиденциальные данные» (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные и просит перевести деньги «на защищённый счет, который закреплён за персональным менеджером — это нужно для безопасности, а потом вы сможете вернуть

900	+7900, +900
8 800 555-55-50	8 800 555-55-51
8 495 500-55-50	8 499 555-55-50

34

Способы обмана

Как обманывают мошенники

СБЕРБАНК

Как защитить себя

• Запишите номера банка в адресную книгу своего телефона:
900, 8 800 555-55-50
• Если звонок будет с другого номера, он отобразится как неизвестный.
• Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.
• Сразу заканчивайте разговор. Работник банка никогда не попросит у вас секретные данные от карты или интернет-банка.
• Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся.

900

8 800 555-55-50

8 495 500-55-50

+7900, +900

8 800 555-55-51

8 499 555-55-50

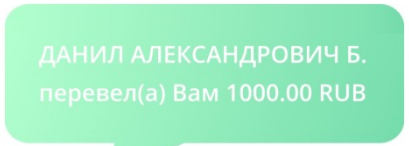
35

Способы обмана

Как обманывают мошенники

СБЕРБАНК

Ситуация 2. «Перевод по ошибке»



Вы оставили своё имя и номер телефона на сайте бесплатных объявлений
Вскоре кто-то присылает вам с мобильного телефона СМС, подделанное под банковское сообщение об операции.
Затем с другого номера приходит СМС с просьбой вернуть деньги.

Мошенники исчезают после перевода
Если вы самостоятельно сделали перевод, деньги вернуть не получится.

Как защитить себя

- Проверьте номер, с которого пришла СМС.
- Помните: банк присылает СМС только с номеров 900 или 9000.
- Проверьте баланс своей карты, чтобы убедиться, действительно ли деньги поступили на счёт.
- Если заподозрили СМС-мошенничество, сразу обратитесь к своему персональному менеджеру или позвоните в банк на номер 900, или на номер, указанный на обратной стороне карты, либо через мобильное приложение СБОЛ.
- Для удобства внешите номера банка в телефонную книгу.

36

Способы обмана

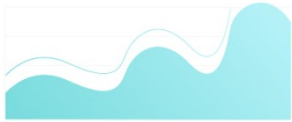
Как обманывают мошенники

СБЕРБАНК

Ситуация 3. «Брокерские или дилерские услуги»

«Выгодные инвестиции»

Вариант 1. Вам звонит незнакомец, который называет себя представителем брокерской или дилерской компании, предлагает инвестировать деньги и обещает высокий доход. Вы соглашаетесь открыть счёт и самостоятельно переводите деньги на карту третьего лица. **Мошенники пропадают, вернуть деньги невозможно.**

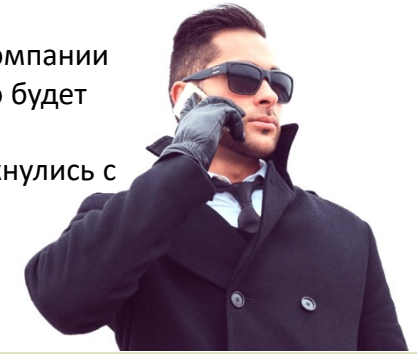


Бинарные опционы

Вариант 2. Вы регистрируетесь на сайте бинарных опционов. После пополнения баланса вы получаете уведомление о получении «бонусных доходов». Чтобы вывести эти деньги, вам нужно повысить «торговый статус». Для этого вы вносите на счёт дополнительную сумму. **Мошенники пропадают, вернуть деньги невозможно.**

Как защитить себя

- Проверьте лицензию. Прежде чем переводить деньги брокерской компании, убедитесь, что у неё есть лицензия. Список компаний с лицензиями на осуществление брокерской или дилерской деятельности есть на сайте Центрального банка РФ.
- Проверьте реквизиты. Реальные брокерские или дилерские компании не просят перевести средства на карту обычного человека — это будет именно счёт компании.
- Позвоните в банк по номеру **900**, если подозреваете, что столкнулись с мошенничеством.



37

Способы обмана

Как обманывают мошенники

СБЕРБАНК

Ситуация 4. «Опрос от Сбербанка»

Вы получаете письмо или СМС о том, что Сбербанк проводит лотерею

Вам предлагают пройти опрос по ссылке, вы кликаете и попадаете на фишинговый сайт.

Фишинг *— это когда у вас пытаются выудить секретную информацию, например, пароль от личного кабинета.*

• Вы проходите «опрос» на сайте, и за это вам обещают крупную сумму вознаграждения, например, 150 тысяч рублей.
• Но для подтверждения карты и перечисления бонусов вас просят перечислить «закрепительный платеж» в размере 150 рублей.
• Вы отправляете деньги, а потом не можете связаться с мошенниками.

Как защитить себя

• Настройте блокировку фальшивых сайтов в своём браузере. Когда оплачиваете покупки в интернете, проверяйте адрес сайта. Если домен не совпадает в точности с официальным названием сайта, не вводите данные.
• Выбирайте защищённое интернет-соединение. Адрес сайта должен начинаться с букв https, а не с http, а в адресной строке должен отображаться значок в виде закрытого замка.
• Подключите СМС-банк. Он понадобится для подтверждения платежа паролем от банка.

38

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Кажется, меня атакуют мошенники. Что делать?

Срочно позвоните в контактный центр Сбербанка на номер **900** (с мобильного телефона) или зайдите в Сбербанк Онлайн, выберите карту и нажмите «Заблокировать карту», после чего позвоните в банк.

Мне пришло СМС о том, что мою карту заблокировали. Что делать?

Посмотрите, с какого номера пришло СМС:

• Если сообщение пришло с номера **900**, позвоните в банк любым удобным способом:

— в контактный центр Сбербанка из мобильного приложения Сбербанк Онлайн

— с мобильного телефона на номер **900**

— или с любого телефона на номер, указанный на обратной стороне карты. Сотрудник банка сообщит вам дальнейшие действия.

• Если сообщение пришло с другого номера, вероятнее всего, его отправили мошенники. Перезванивать на этот номер «для разблокировки» нельзя. Если появились сомнения, действительно ли ваша карта заблокирована, вы можете позвонить в банк по номеру **900** и уточнить информацию.

39

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Мне пришло СМС о том, что по моей карте проведена операция, но я эту операцию не совершал. Что делать?

Если вы зарегистрированы в Сбербанк Онлайн, проверьте последние операции в своем личном кабинете или мобильном приложении. Если там нет такой операции, напишите нам прямо сейчас. После этого удалите СМС. Если же вы действительно видите такую операцию в истории операций, но не совершали её, позвоните в банк любым удобным способом: — в контактный центр Сбербанка из мобильного приложения Сбербанк Онлайн — с мобильного телефона на номер **900** — или с любого телефона на номер, указанный на обратной стороне карты.

Мне пришло СМС с номера 9000, а не 900. Это мошенники?

Нет. С номера **9000** Сбербанк проводит СМС-опрос о качестве обслуживания и проводит актуализацию данных. СМС-опрос оплачивается по тарифному плану клиента. Сообщение может содержать ссылку на опрос Сбербанка opros.sberbank.ru или на портал Центра недвижимости Сбербанка Domclick.ru

40

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Что делать, если я потерял или у меня украли телефон, к которому подключён СМС-банк?

В этой ситуации вам нужно обратиться в банк и попросить временно заблокировать СМС-банк. Затем заблокируйте свою сим-карту у сотового оператора.

Мне позвонил сотрудник службы безопасности Сбербанка и сообщил о попытках неизвестных лиц снять деньги с моей карты. Могу ли я сообщать ему номер моей карты?

Если вам звонит сотрудник банка, он не будет запрашивать номер вашей карты, ПИН-код или CVV2/CVC2-код, логин, пароль от Сбербанк Онлайн или код из СМС. В этой ситуации прекратите разговор и позвоните в банк любым удобным способом:

— в контактный центр Сбербанка из мобильного приложения Сбербанк Онлайн,
— с мобильного телефона на номер **900**,
— или с любого телефона на номер, указанный на обратной стороне карты.

41

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Как определить, что мне звонит именно сотрудник банка, а не злоумышленник?

При звонке клиенту сотрудник Сбербанка всегда обращается по имени-отчеству; никогда не просит конфиденциальные сведения: полные реквизиты карты (номер карты, ПИН- и CVV-код), СМС-пароли банка; никогда не требует совершать операций с картой. Помните, что задача мошенника — застать вас врасплох и не дать времени проанализировать ситуацию, поэтому он будет настаивать, чтобы вы выполнили его требования как можно быстрее.

Могу ли я пользоваться банкоматом, если он зависает, самопроизвольно перезагружается или на экране появляются подозрительные изображения?

Таким банкоматом пользоваться нельзя. Отмените текущую операцию, нажав кнопку «Отмена», и дождитесь возврата карты. Если банкомат не возвращает карту, позвоните на номер 900 или по телефону, указанному на банкомате. Не отходите от банкомата, пока не выполните рекомендации сотрудника банка.

42

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Что делать, если банкомат не возвращает карту?

Позвоните на номер **900** или по телефону, указанному на банкомате. Не отходите от банкомата, пока не выполните рекомендации сотрудника банка.

Мне пришло с незнакомого номера СМС о том, что на мой счет переведены деньги. А потом мне пришло СМС с просьбой их вернуть, так как деньги перевели по ошибке. Я могу вернуть деньги?

Сбербанк отправляет СМС только с номера **900** или **9000**, сообщения о совершенных операциях с других номеров совершают, как правило, мошенники. Если вам пришло СМС с другого номера, напишите нам в форме обратной связи и перешлите нам текст СМС. После этого удалите СМС.

Мне пришла ссылка на установку мобильного приложения Сбербанк Онлайн. Я могу его установить?

Нет, устанавливать приложения по ссылкам из СМС-сообщений или электронной почты нельзя, даже если в сообщении утверждается, что оно из банка. Используйте только официальные приложения банка для Android, iPhone, iPad и Windows Phone.

43

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Для входа в интернет-банк Сбербанк Онлайн у меня запрашивают номер банковской карты. Я могу его ввести?

Нет. Для входа в Сбербанк Онлайн нужен только логин, личный пароль или одноразовый пароль из СМС. Если на сайте запрашивают любую другую персональную информацию, например, номер банковской карты или мобильного телефона, покиньте сайт и срочно обратитесь в банк.

Мне предложили продать мою банковскую карту. Очень выгодное предложение, я могу на него согласиться?

Не соглашайтесь, её могут использовать в мошеннических целях. Правоохранительные органы в первую очередь будут проверять владельца карты на причастность к преступлению.

44

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Мне пришло подозрительное письмо на электронную почту. Как понять, мошенничество это или нет?

В первую очередь обратите внимание на почту отправителя. Как правило, мошенники используют общедоступные почтовые домены или покупают домены, похожие на официальные доменные имена компаний, чтобы ввести получателя письма в заблуждение.
Вас должно насторожить, если тема, контент письма или название файлов побуждают вас к немедленному действию: перейти по ссылке, нажать на кнопку, открыть файл, немедленно ответить на письмо.

Важно также обратить внимание на обращение и подпись в письме: если они безличные, высока вероятность обмана. Контакты для обратной связи в таком письме могут быть недостоверны, поэтому проверьте их на официальном сайте компании.
Не переходите по ссылкам и не кликайте на подозрительные объекты. Наведите курсор мыши на подозрительную ссылку или объект, чтобы увидеть, куда она ведёт на самом деле. Сравните адрес с адресом официального сайта компании.
Будьте осторожны с вложениями: открывайте только те из них, которые вы ждали от своих адресатов.
Не вводите свои конфиденциальные данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы.
Не отвечайте на подозрительные письма.

45

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

При оплате покупки на сайте я ввел номер своей карты и CVV. Мне написали, что произошла ошибка и для отмены операции меня просят сообщить СМС-код. Можно ли мне его отправить?

Нет. Никогда не вводите «пароли для отмены операции» и не сообщайте никому СМС-коды. Об этом могут попросить только мошенники. Если вы с этим столкнулись, покиньте сайт и срочно обратитесь в банк.

Мне пришло сообщение о том, что Сбербанк проводит лотерею и предлагает пройти опрос. Я перешёл по ссылке, ответил на вопросы, и теперь меня ждет приз. Могу ли я подтвердить свою карту и произвести «закрепительный платёж» для перечисления вознаграждения?

Ни в коем случае. Это распространенная схема мошенничества, когда от имени банка мошенники направляют ссылки на фишинговые сайты. Не переходите по подозрительным ссылкам, при любой оплате в интернете проверяйте адрес сайта и вводите данные только если домен точно совпадает с официальным названием сайта.

46

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Я стал свидетелем мошенничества. Что делать?

Напишите по адресу fraud@sberbank.ru , если стали свидетелем любой мошеннической деятельности, например:
если вы обнаружили сайт с сомнительными финансовыми предложениями,

где мошенники скрываются под брендом Сбербанка и вводят в заблуждение потребителей;

если вам пришло подозрительное СМС сообщение, якобы от банка,

о проведении операции и требованием позвонить;

если вам звонили мошенники и пытались получить персональные данные;

если вы получили сомнительное письмо, возможно содержащее вирус или ссылку на источник распространения вируса;

если вам известны номера карт, используемые мошенниками для хищения денег;

если вы обнаружили уязвимость на одном из публичных онлайн-сервисов Сбербанка: Сбербанк Онлайн, Сбербанк Бизнес Онлайн, сайт sberbank.ru и других.

47

Популярные вопросы

Ответы на популярные вопросы

СБЕРБАНК

Я потерял свою банковскую карту. Что мне делать?

Если вы потеряли карту или подозреваете, что ваш счёт атакуют мошенники, срочно её заблокируйте. Для этого позвоните в контактный центр Сбербанка на номер **900** с мобильного телефона. Или зайдите в интернет-банк или мобильное приложение Сбербанк Онлайн — найдите нужную карту и нажмите «Заблокировать»

СБЕРБАНК
Всегда рядом

Благодарим за внимание!