Toyota
Financial Services

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

ОГЛАВЛЕНИЕ

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

1. О КИБЕРМОШЕННИЧЕСТВЕ И ЕГО ОПАСНОСТИ

Актуальность темы и риски для клиентов банка

С каждым годом кибермошенничество становится всё более сложным и изощрённым, что создаёт серьёзную угрозу для банковских клиентов. Современные технологии облегчают доступ к финансовым услугам и в то же время создают благоприятные условия для злоумышленников. Киберпреступники используют социальную инженерию, фишинг, вирусы и мошеннические сайты для хищения личных данных, паролей и финансовых средств. В результате клиенты могут потерять свои сбережения, подвергнуться кредитным аферам или стать жертвами кражи личности.

Для банка важно не только обеспечить высокую степень защиты своих систем, но и обучить клиентов правильному поведению в цифровой среде. Безопасность – вопрос не только технологий, но и осведомлённости самих пользователей.

Цель памятки

Данная памятка создана для того, чтобы повысить осведомлённость клиентов банка о рисках кибермошенничества и научить их защищать свои финансовые данные. В памятке представлены основные виды мошенничества, признаки подозрительных действий и рекомендации по безопасному использованию онлайн-банкинга и мобильных приложений. Следуя этим рекомендациям, клиенты смогут свести к минимуму вероятность стать жертвой киберпреступников.

2. МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

Примеры мошенничества через личные сообщения или объявления

Социальные сети и мессенджеры стали популярной платформой для мошенников, т. к. эти каналы позволяют легко устанавливать контакт с потенциальными жертвами и использовать социальную инженерию. Мы собрали самые распространённые схемы мошенничества через эти платформы.

- **Мошенничество с «продажами» или «покупками».** Мошенники размещают фальшивые объявления о продаже товаров или услуг по очень привлекательным ценам. После получения предоплаты они исчезают, не отправляя товар. Часто используется поддельная информация, например, фальшивые профили с украденными фотографиями.
  Пример: вы видите объявление о продаже смартфона по очень низкой цене и переводите деньги продавцу, но товар так и не получаете.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

- **Фальшивые розыгрыши и конкурсы.** В социальных сетях появляются фальшивые розыгрыши, где мошенники предлагают пользователям выиграть дорогие призы. Для участия вас просят перейти по ссылке и ввести данные банковской карты или другую конфиденциальную информацию.
  Пример: пост в социальной сети утверждает, что вы выиграли автомобиль, и для получения приза нужно оплатить «регистрационный сбор».

- **Фишинг через мессенджеры.** Мошенники отправляют личные сообщения от имени ваших друзей или знакомых, утверждая, что им срочно нужна помощь (например, деньги или реквизиты для перевода). Часто мошенники взламывают чужие аккаунты и используют доверие жертвы к своему другу или родственнику.
  Пример: вы получаете сообщение от друга с просьбой помочь в экстренной ситуации и одолжить деньги, но на самом деле это не ваш друг, а злоумышленник, взломавший его аккаунт.

- **Мошенничество с инвестициями.** Мошенники предлагают жертве поучаствовать в «выгодных инвестиционных проектах», обещая быстрый и высокий доход. Жертва обмана переводит деньги на счёт «для старта», но после перевода мошенники исчезают.
  Пример: вы получаете сообщение в мессенджере от неизвестного человека, предлагающего вложить деньги в криптовалюту с гарантированной прибылью, но на самом деле это мошенничество.

- **Поддельные благотворительные сборы.** Злоумышленники создают фальшивые страницы благотворительных организаций и просят пожертвовать средства для помощи больным детям, пострадавшим в катастрофах, или животным. Деньги в итоге попадают не к нуждающимся, а к мошенникам.
  Пример: вы видите пост с просьбой о срочной помощи больному ребёнку с ссылкой на оплату через мессенджер, но вся собранная сумма достаётся мошенникам.

Советы и рекомендации как защитить свои данные и деньги от мошенничества в социальных сетях и мессенджерах

- **Будьте осторожны с личными сообщениями.**
  Никогда не передавайте личные данные, реквизиты карт или пароли в ответ на личные сообщения, даже если они приходят от ваших знакомых. Если получаете подозрительное сообщение от друга, позвоните ему напрямую для подтверждения.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

- **Проверяйте подлинность страниц и объявлений.**
  - Всегда проверяйте профили пользователей, размещающих объявления, и ищите отзывы других покупателей. Если что-то кажется слишком хорошим, чтобы быть правдой, это, скорее всего, мошенничество.
  - Используйте официальные площадки для покупок и проверяйте репутацию продавцов.

- **Относитесь с осторожностью к «выгодным» предложениям.**
  Мошенники часто обещают невероятные доходы или выгодные покупки. Будьте предусмотрительны по отношению к предложениям, требующим срочных решений и быстрых переводов денег.

- **Не переходите по подозрительным ссылкам.**
  Мошенники часто используют сокращённые или замаскированные ссылки. Не переходите по ссылкам из подозрительных сообщений и не устанавливайте приложения по запросу неизвестных лиц.

- **Проверяйте благотворительные организации.**
  Прежде чем сделать пожертвование, проверьте подлинность организации на официальных сайтах и убедитесь, что она зарегистрирована. Никогда не переводите деньги напрямую на личные счета незнакомцев.

- **Установите многофакторную аутентификацию.**
  Используйте двухфакторную аутентификацию для своих аккаунтов в социальных сетях и мессенджерах, чтобы защитить их от взлома. Это повысит уровень безопасности.

- **Сообщайте о подозрительных действиях.**
  Если вы столкнулись с мошенничеством или видите подозрительные объявления и сообщения, сообщите об этом в службу поддержки социальной сети или мессенджера.

АО «Тойота Банк» напоминает, что личные данные, реквизиты банковских карт и другие конфиденциальные сведения не должны передаваться через социальные сети и мессенджеры, т. к. это самые уязвимые каналы для мошенничества.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

3. ПОДДЕЛЬНЫЕ БАНКОВСКИЕ САЙТЫ И ПРИЛОЖЕНИЯ

Как мошенники подделывают банковские ресурсы

Мошенники часто создают поддельные сайты и мобильные приложения, которые выглядят как официальные ресурсы банков, чтобы обмануть пользователей и получить доступ к их конфиденциальной информации, такой как логины, пароли или данные банковских карт. Злоумышленники используют разные методы для создания таких фальшивок.

- **Копирование дизайна.** Поддельные сайты и приложения почти полностью копируют внешний вид официальных банковских ресурсов. Логотипы, цветовая схема, шрифты и структура страницы или интерфейса выглядят идентично оригиналу, что затрудняет их распознавание обычными пользователями.

- **Изменение доменных имён.** Мошенники регистрируют домены, которые очень похожи на официальные, но содержат незначительные изменения, например, добавление или замена одной буквы или цифры (вместо bank.com – banq.com и т. п.). При беглом просмотре пользователь не заметит подвоха.

- **Рассылка фишинговых писем и сообщений.** Для того чтобы заманить пользователей на поддельные сайты, мошенники рассылают электронные письма или СМС-сообщения с ссылками на такие сайты. В этих сообщениях может содержаться информация о необходимости обновить данные, подтвердить транзакцию или решить проблему со счётом.

- **Создание поддельных приложений.** Мошенники размещают в сторонних магазинах приложений и даже в официальных маркетах фальшивые мобильные приложения, имитирующие официальные банковские. Эти приложения могут запрашивать у пользователей данные для входа в их учётные записи или реквизиты карт, а затем передавать их злоумышленникам.

- **Использование вредоносного ПО.** Некоторые фальшивые банковские приложения могут содержать вредоносное программное обеспечение, которое получает доступ к устройству пользователя, перехватывает данные или отправляет информацию злоумышленникам.

Советы как проверить подлинность сайта и приложения

- **Проверяйте адреса сайта.**
  - Всегда внимательно проверяйте URL сайта. Официальные банковские сайты обычно используют защищённые соединения (https://) и доменные имена,

которые легко узнать. Если в адресе присутствуют лишние символы, буквы или доменные зоны, отличные от оригинальных, этот сайт может быть поддельным.

– Проверьте наличие замка или индикатора защищённого соединения в адресной строке браузера, свидетельствующего о наличии SSL-сертификата. Это не всегда гарантирует безопасность, но существенно её повышает.

- **Используйте официальные ссылки.**
Всегда переходите на сайт банка через сохранённые закладки или вводите адрес вручную, не используйте для этого ссылки из писем или сообщений. Фишинговые ссылки могут выглядеть убедительно, но приведут вас на фальшивую страницу. Официальный адрес АО «Тойота Банк» https://toyota-bank.ru

- **Скачивайте приложения только из официальных магазинов.**
  – Устанавливайте банковские приложения только из официальных источников, таких как Google Play или App Store. Избегайте установки приложений через сторонние сайты или ссылки в СМС-сообщениях и электронных письмах.
  – Перед установкой проверьте разработчика приложения – он должен быть указан как официальный банк. Читайте отзывы и обращайте внимание на количество загрузок, поскольку поддельные приложения могут иметь мало отзывов и/или низкие оценки.

- **Проверяйте информацию на сайте.**
  – Убедитесь, что все ссылки, разделы и страницы сайта работают корректно. Мошеннические сайты часто могут иметь нерабочие или неправильно ведущие ссылки.
  – Если сайт просит ввести слишком много личных данных, которые обычно не требуются при стандартных операциях, это сигнал для дополнительной проверки сайта на мошенничество.

- **Используйте многофакторную аутентификацию.**
Подключите двухфакторную аутентификацию (2FA) в своём банке. Это добавит ещё один уровень защиты к вашему аккаунту, даже если кто-то узнает ваши логин и пароль.

- **Проверяйте сертификаты безопасности.**
В браузере можно посмотреть сертификат безопасности сайта, который должен быть выдан авторитетной организацией. Если сайт вызывает сомнения, лучше воздержаться от ввода личных данных.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

- **Сообщайте о подозрительных приложениях и сайтах.**
  Если вы заметили подозрительный сайт или приложение, немедленно сообщите об этом в службу поддержки вашего банка и прекратите любое взаимодействие с ресурсом.

- **Обновляйте приложения и операционные системы.**
  Регулярно обновляйте операционную систему вашего устройства и все установленные приложения, чтобы избежать уязвимостей, которые могут быть использованы мошенниками.

Следуя этим рекомендациям, можно существенно снизить риск стать жертвой мошенников, которые подделывают банковские сайты и приложения.

4. МОШЕННИЧЕСТВО С КАРТАМИ И ИНТЕРНЕТ-ПЛАТЕЖАМИ

Методы кражи данных карт

Злоумышленники используют различные методы для кражи данных банковских карт, чтобы осуществлять несанкционированные платежи и переводы.

- **Скимминг**
  Скиммеры – устройства, устанавливаемые на банкоматы или терминалы оплаты для считывания данных с магнитной полосы карты. Часто мошенники используют скрытые камеры или накладки на клавиатуру для записи введённого ПИН-кода. Это позволяет им клонировать карту и получить доступ к деньгам жертвы.

- **Шимминг**
  Современная версия скимминга, при которой используется миниатюрное устройство для перехвата данных с чипа карты. Хотя данные чипа сложнее подделать, некоторые виды атак позволяют частично использовать информацию для кражи средств.

- **Фишинг и вишинг**
  Мошенники рассылают электронные письма, сообщения или звонят жертвам, представляясь сотрудниками банка, с целью получить данные карты, ПИН-код или код CVV. Жертва может не осознавать, что её обманули, пока не произойдёт списание средств.

- **Перехват данных при интернет-платежах**
  Злоумышленники могут использовать фальшивые сайты, заражённые компьютеры или вредоносное ПО для перехвата данных карт при совершении онлайн-транзакций.

- **Вредоносное ПО (кейлоггеры)**
  Кейлоггеры записывают нажатия клавиш на устройстве жертвы, в том числе ввод данных карты при интернет-платежах. Эти данные затем передаются мошенникам.

- **Мошенничество с участием дропперов**
  Дропперы – подставные лица, которых мошенники используют для обналичивания украденных средств. Дроппер может получать либо деньги на свои банковские счета или карты, либо товары, купленные на украденные средства, а затем передавать их мошенникам за небольшую компенсацию. Часто дропперы не осознают, что участвуют в преступной схеме, и их могут использовать для запутывания следов финансовых операций.

  Мошенники могут привлекать дропперов через объявления о «быстром заработке», не объясняя, что деньги получены незаконным путём. В некоторых случаях дропперов могут привлекать через соцсети или мессенджеры, предлагая «работу с переводами денег».

- **Банкоматы и терминалы с компрометированным ПО**
  Иногда злоумышленники устанавливают вредоносное ПО на банкоматы и терминалы для записи данных карт при транзакциях. Такие устройства могут перехватывать данные и передавать их мошенникам.

5. КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ ПРИ ОПЛАТЕ ОНЛАЙН

Для того чтобы защитить данные своей карты в Интернете, следует соблюдать правила безопасного использования банковских карт онлайн.

- **Используйте карты с технологией 3D Secure.**
  Это дополнительная защита для интернет-платежей, при которой требуется ввод одноразового пароля, отправленного на телефон владельца карты. Если интернет-магазин поддерживает 3D Secure, злоумышленники не смогут завершить транзакцию без этого кода.

- **Платите только на проверенных сайтах.**
  Убедитесь, что сайт защищён (URL начинается с https://, есть значок замка в адресной строке). Избегайте покупок на сомнительных или малоизвестных сайтах.

- **Используйте виртуальные карты для интернет-платежей.**
  Для интернет-покупок безопаснее использовать одноразовые виртуальные карты, которые можно пополнять на конкретные суммы. Это ограничит возможность кражи данных основной карты.

Toyota Financial Services

- **Подключите уведомления о транзакциях.**
  Включите уведомления о каждой транзакции по СМС-сообщению или в банковском приложении. Это позволит вовремя обнаружить несанкционированные операции и немедленно заблокировать карту.

- **Не храните данные карт на сайтах и в браузерах.**
  Не сохраняйте реквизиты карт в онлайн-магазинах и браузерах, особенно на чужих устройствах. Даже если сайт предлагает надёжное сохранение для будущих покупок, лучше вводить данные каждый раз заново.

- **Используйте сложные пароли и двухфакторную аутентификацию.**
  Сложные пароли для аккаунтов в интернет-магазинах и платёжных системах и двухфакторная аутентификация (например, через СМС-сообщения) обеспечат дополнительную защиту.

- **Проверяйте выписки по карте.**
  Регулярно просматривайте банковские выписки и проверяйте все транзакции. При обнаружении подозрительной операции свяжитесь с банком и заблокируйте карту.

- **Установите антивирусное ПО.**
  Антивирус поможет защитить устройство от вредоносного ПО, которое может перехватывать данные карт.

- **Не совершайте платежи через публичные Wi-Fi-сети.**
  Осуществляйте интернет-платежи только через безопасные сети. Публичные Wi-Fi-сети могут быть уязвимы для перехвата данных.

- **Относитесь с осторожностью к предложениям «лёгкого заработка».**
  Никогда не соглашайтесь на предложения, связанные с использованием вашего банковского счёта или карты для получения переводов и отправки товаров. Это схема может быть мошеннической с участием дропперов, и в результате вы можете оказаться вовлечённым в уголовное дело.

Эти советы помогут защитить ваши банковские карты и данные от мошенников, а также снизить риск утраты средств при оплате в Интернете.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

6. МОШЕННИЧЕСТВО С ИНВЕСТИЦИЯМИ И ФИНАНСОВЫЕ ПИРАМИДЫ

Как распознать подозрительные предложения по вложению средств

Мошенничество с инвестициями и финансовые пирамиды являются одними из самых распространённых схем обмана. Мошенники обещают высокие прибыли с минимальными рисками, привлекая людей к вложению денег в фальшивые или ненадёжные проекты. Для того чтобы не стать жертвой подобных схем, важно уметь распознавать признаки мошенничества.

- **Обещание высокой доходности без риска**
  Один из основных признаков финансового мошенничества – обещание больших доходов с минимальными или нулевыми рисками. Реальные инвестиционные инструменты всегда связаны с определённой степенью риска. Если предложение звучит слишком хорошо, чтобы быть правдой, оно, скорее всего, мошенническое.

- **Давление со стороны организаторов**
  Мошенники часто создают ощущение срочности, убеждая потенциальных жертв, что предложение ограничено по времени или доступно только для избранных. Они могут использовать тактики давления, чтобы заставить вас быстро принять решение, не давая времени на анализ.

- **Неясные или сложные схемы инвестирования**
  Если вы не можете понять, каким образом будет происходить заработок на инвестициях, это повод для подозрений. Мошенники часто скрывают реальную суть своего предложения за сложными и неясными финансовыми схемами, которые никто не может объяснить доступным языком.

- **Отсутствие лицензий и регистрации**
  Настоящие инвестиционные компании должны быть зарегистрированы и лицензированы в соответствующих органах (например, Центральном банке России). Если организация не может предоставить информацию о своей регистрации или лицензии, это явный признак мошенничества.

- **Система вознаграждения за привлечение новых участников**
  Финансовые пирамиды часто основываются на привлечении новых участников. Вложив деньги, вы получаете вознаграждение только в том случае, если приведёте других людей, которые тоже вложат средства. Такая схема не является законной инвестицией и рано или поздно развалится, оставив большинство участников без денег.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

- **Отсутствие прозрачности**
  Мошенники избегают прозрачности в своих действиях: они не предоставляют полных и понятных отчётов о движении средств, инвесторах и операциях. Если компания не готова раскрыть информацию о том, как управляются ваши деньги, это серьёзный сигнал для отказа от сотрудничества.

- **Использование эмоциональных манипуляций**
  Злоумышленники могут апеллировать к чувству страха или жадности, рассказывая о возможных финансовых потерях, если вы не вложите средства, или, напротив, обещая вам финансовую независимость и успех.

- **Фиктивные отчёты о доходности**
  Мошенники могут показывать вам фальшивые отчёты о том, сколько вы якобы заработали. Это – способ поддерживать у вас иллюзию прибыли и мотивировать к дальнейшим вложениям, тогда как в реальности доходов нет.

Как проверить надёжность инвестиционного предложения

- **Проверьте компанию в реестре ЦБ.**
  Все организации, предлагающие финансовые услуги, включая инвестиции, должны быть зарегистрированы и иметь лицензию от Центрального банка. На официальном сайте ЦБ можно проверить, зарегистрирована ли компания и обладает ли она необходимыми разрешениями для ведения инвестиционной деятельности.

- **Изучите документы компании.**
  Прежде чем вкладывать деньги, запросите у компании все необходимые документы, такие как регистрационные данные, лицензии, финансовые отчёты и условия договора. Любая легальная инвестиционная компания обязана предоставить эту информацию по запросу.

- **Проверьте отзывы и репутацию.**
  Изучите отзывы других клиентов и информацию о компании в открытых источниках. Если негативных отзывов, жалоб на невыплаты или затягивание операций много, это повод насторожиться.

- **Проверьте сайт компании.**
  Надёжная инвестиционная компания должна иметь профессиональный сайт с полным набором юридической и контактной информации. Обратите внимание на наличие данных о руководстве компании, адресах и контактных телефонах. Если контактная информация минимальна или отсутствует, это повод задуматься.

- **Избегайте анонимных или офшорных компаний.**
  Мошенники могут предложить вложить средства в анонимные или зарегистрированные в офшорах компании, чтобы уклониться от регулирования и ответственности. Отсутствие прозрачности в юрисдикции – сигнал для отказа от инвестиций.

- **Оцените реалистичность предложения.**
  Оцените, насколько реалистичны обещанные доходы и сроки. Предложения по повышению доходности значительно выше рыночной при отсутствии чётких объяснений, как она будет достигнута, должны насторожить вас.

- **Не вкладывайте все средства в одну компанию.**
  Даже если предложение выглядит надёжным, никогда не инвестируйте все свои сбережения в один проект. Разделение вложений на несколько инвестиционных инструментов позволит снизить риски потерь.

- **Консультируйтесь с независимыми экспертами.**
  Прежде чем принять решение о крупном вложении, обратитесь за консультацией к независимым финансовым советникам. Это поможет оценить риски и избежать участия в сомнительных схемах.

- **Помните об ответственности.**
  Важно понимать, что каждый инвестор несёт ответственность за свои решения. Рекомендуется избегать эмоциональных покупок и не вкладывать деньги в предложения, которые вызывают сомнения, или если на вас оказывают давление.

Следование этим рекомендациям позволит минимизировать риск попадания в ловушку мошенников и даст возможность принимать взвешенные инвестиционные решения.

Если вы стали жертвой мошенников, важно действовать быстро и последовательно.

- **Блокировка карт и счетов**
  Немедленно свяжитесь с вашим банком или финансовым учреждением и заблокируйте все пострадавшие карты и счета. Это поможет предотвратить дальнейшие несанкционированные транзакции.

- **Обращение в банк**
  Уведомите свой банк о произошедшем инциденте. Попросите их предоставить информацию о том, как можно вернуть украденные средства и какие дополнительные меры безопасности можно предпринять.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

- **Подача заявления в полицию**
  Напишите заявление в полицию. Обязательно сохраните копию заявления и любые другие документы, связанные с инцидентом. Это может быть полезно в случае дальнейших расследований и для возмещения убытков.

- **Уведомление о мошенничестве**
  Если ваши личные данные были скомпрометированы, уведомите о мошенничестве соответствующие организации, такие как кредитные бюро, чтобы предотвратить возможные случаи мошенничества в будущем.

Советы по восстановлению контроля после инцидентов

- **Контроль за кредитной историей**
  Регулярно проверяйте свою кредитную историю на наличие подозрительных или несанкционированных записей. Это поможет своевременно обнаружить возможное мошенничество.

- **Использование антивирусного ПО и обновлений**
  Убедитесь, что на всех ваших устройствах установлено актуальное антивирусное ПО и что оно регулярно обновляется.

- **Изменение паролей**
  Измените пароли во всех ваших учётных записях, особенно тех, которые могли быть скомпрометированы. Используйте сложные и уникальные пароли для каждой учётной записи.

- **Оповещение о подозрительной активности**
  Следите за подозрительной активностью на своих финансовых счетах и немедленно сообщайте о любых аномалиях в ваш банк.

- **Психологическая поддержка**
  Психологическое воздействие от мошенничества может быть значительным. Не стесняйтесь обращаться за поддержкой к специалистам, если чувствуете необходимость.

Предприняв эти действия, вы сможете минимизировать ущерб и восстановить контроль над вашей финансовой безопасностью.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

7. ПОЛЕЗНЫЕ КОНТАКТЫ

Мошенничество – серьёзная угроза, с которой может столкнуться каждый. Чтобы минимизировать риски и быстрее восстановиться после инцидента, важно знать основные правила личной финансовой безопасности, а также иметь под рукой контакты, которые могут быть полезны в случае мошенничества. Осведомлённость о мерах безопасности и профилактических действиях – залог защиты от киберугроз.

Полезные контакты

- **Полиция**
  Номер для вызова: 102

- **Центральный банк России**
  Официальный сайт: https://www.cbr.ru/
  Контактный центр: 8-800-300-30-00
  На сайте Центробанка также есть информация о действиях в случае мошенничества.

- **Контакты АО «Тойота Банк»**
  Официальный сайт: https://toyota-bank.ru
  Контактный центр: 8-800-200-08-40

8. ДОПОЛНИТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ

- **Локальные ресурсы по кибербезопасности**
  В России это, например, портал «Стопмошенник.рф», где представлены актуальные схемы мошенничества и рекомендации как защититься от них.

- **Социальные сети и рассылки банков**
  Многие банки и финансовые организации ведут блоги и каналы в социальных сетях, где делятся полезными советами по безопасности.

Следуя этим рекомендациям и обращаясь к надёжным источникам, вы сможете повысить свою защиту и быть готовым к любым инцидентам.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

9. ОТВЕТЫ НА ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Как юридическому лицу, индивидуальному предпринимателю и лицу, которое занимается частной практикой, обжаловать включение реквизитов в базу данных «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента»?

Это возможно одним из двух способов:

– обратиться с заявлением в любой из банков, в котором обслуживаетесь вы или ваша компания. Банк обязан перенаправить обращение клиента в Банк России не позднее следующего рабочего дня (при отсутствии основания для отказа в передаче заявления в Банк России);

– направить заявление в Банк России через интернет-приемную, выбрав в качестве темы обращения «Информационную безопасность» и соответствующий тип проблемы.

Независимо от способа обращения индивидуальному предпринимателю и лицу, которое занимается частной практикой, в заявлении нужно обязательно указать следующие данные:

– серию (при наличии) и номер документа, удостоверяющего личность;

– ИНН;

– номера банковских счетов и/или платежных карт, и/или электронных кошельков.

Дополнительно вы можете указать в заявлении полные и сокращённые (при наличии) наименования банков, от которых вы узнали о включении сведений в базу данных Банка России, и/или их банковские идентификационные коды, а также номер телефона.

Юридическому лицу в заявлении нужно обязательно указать следующие данные:

– ИНН;

– номера банковских счетов и/или платежных карт, и/или электронных кошельков.

Кроме того, если банк полагает, что сведения о его клиенте включены в базу данных необоснованно, то он вправе самостоятельно, без участия клиента, направить в Банк России мотивированное заявление.

Банк России в течение 15 рабочих дней рассмотрит заявление и примет решение о целесообразности исключения реквизитов из базы данных.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Как человек или компания узнают о вынесенном Банком России решении по результатам рассмотрения заявления об исключении сведений из базы данных?

Банк России в течение 15 рабочих дней рассмотрит заявление и примет решение о целесообразности исключения реквизитов из базы данных.

Если клиент обращался с заявлением в свой банк, то решение регулятора будет направлено в адрес банка. При этом ответ Банка России кредитная организация обязана сообщить клиенту не позднее следующего рабочего дня.

В случае когда клиент банка обращался напрямую в Банк России, решение регулятора будет направлено клиенту.

Если банк самостоятельно инициировал процесс обжалования (без участия клиента), то решение регулятора будет направлено в банк.

Может ли сотрудник Банка России звонить через мессенджеры?

Сотрудники Банка России, а также государственных и правоохранительных органов никогда не звонят через мессенджеры. Так поступают мошенники, которые представляются в том числе сотрудниками Банка России. Иногда злоумышленники направляют в мессенджер или на электронную почту поддельное удостоверение с логотипом и печатью Банка России. Такие документы могут содержать имена реальных сотрудников, сведения о которых мошенники получают на сайте регулятора или каким-либо другим способом. Высылая фальшивое удостоверение, они рассчитывают добиться доверия, чтобы потом обманом выманить у человека деньги или оформить на него кредит.

Если вам позвонили якобы работники Банка России или правоохранительных органов и разговор касается ваших финансов, положите трубку. Никогда не переводите деньги и не сообщайте свои личные и финансовые данные по просьбе незнакомого абонента, кем бы он ни представился.

Звонят из банка и сообщают, что кто-то пытается оформить кредит на моё имя. Что делать?

Это – мошенники, поэтому немедленно прервите разговор несмотря на угрозы и давление. Чтобы войти в доверие, злоумышленники могут обращаться по имени и отчеству. Не поддавайтесь на такие уловки. Не совершайте каких-либо действий по счёту, если вам звонят с просьбой или требованием о переводе денег или с предложением об оформлении кредита. Самостоятельно позвоните в банк

по номеру телефона, указанному на его официальном сайте или на обратной стороне карты. Также сообщите своим родственникам или людям, которым вы доверяете, о попытке мошенников обмануть вас.

Мне позвонили из полиции и сообщили, что мои персональные данные были скомпрометированы, а деньги могут быть похищены, и предлагают перевести их на специальный счёт в Центробанке. Что делать?

Это наиболее распространённая мошенническая схема. Не существует «специальных», «безопасных», «защищённых» или каких-либо других счетов, на которые граждане должны переводить деньги в адрес Центрального банка. Злоумышленники упоминают якобы специальный счёт в Центробанке, чтобы усыпить бдительность человека. На самом деле счёт, реквизиты которого называют мошенники, принадлежит им. Не совершайте никаких действий по своему счёту, положите трубку. Если у вас остались какие-либо сомнения, самостоятельно позвоните в банк по номеру телефона, который указан на оборотной стороне карты или на официальном сайте банка.

Как защититься от кибермошенников?

Кибермошенники обманывают людей в Интернете или по телефону. У них множество легенд и способов обмануть человека, которые всегда сводятся к одному: у человека пытаются выманить данные карты, пароли или коды из СМС-сообщений либо провоцируют самостоятельно перевести деньги. Поэтому важно помнить: никогда не сообщайте данные своей карты, пароли из СМС-сообщений, не переводите деньги на счёт по просьбе неизвестного абонента, кем бы он ни представился. Также никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС-сообщения, а лучше – никогда не переходите на сайты по ссылкам из подозрительных писем.

Что делать, если кто-то по ошибке зачислил на мой счёт деньги?

Если вам приходит СМС-сообщение о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем вам звонит человек, который по ошибке зачислил деньги, и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС-сообщение – не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счёта, прежде чем переводить кому-либо деньги; если поступление всё же было, обратитесь в свой банк и сообщите об этом. Банк должен сам вернуть ошибочно зачисленные деньги.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota
Financial Services

Что делать, если приходит сообщение о необходимости подтвердить покупку, которую я не совершал?

Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздаётся звонок от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас данные, чтобы списать с вашего счёта средства или подписать вас на ненужный платный сервис. Если вы получили сообщение о необходимости подтвердить покупку – игнорируйте его.

Что делать, если мне звонят из МВД, ФСБ или других правоохранительных органов и просят данные карты или перевести деньги?

Если вам звонят из банка, полиции или другой организации и просят совершить финансовые операции по счёту (перевод, зачисление, в т. ч. на «безопасный» счет, и т. д.), немедленно прекратите разговор. Если есть сомнения, позвоните в свой банк и узнайте, всё ли в порядке с деньгами.

Зачастую злоумышленники представляются не только «службой безопасности банка», но и «сотрудниками МВД» или других правоохранительных органов, используют разнообразные приёмы, сообщают, например, о якобы проводимых в данный момент мероприятиях по поимке преступников. Будьте бдительны, игнорируйте требования позвонившего. Настоящие сотрудники правоохранительных органов или банка никогда не будут запрашивать у вас данные карты или просить перевести деньги.

Мне на электронную почту пришло письмо от Банка России, в котором говорится о поступлении на моё имя крупной денежной суммы в иностранном банке, и что я должен оплатить комиссию за её получение. Что это?

Банк России по своей инициативе не направляет гражданам письма, не звонит и не рассылает сообщения. При получении электронных писем о поступлении на ваше имя крупной денежной суммы в иностранном банке или организации, происхождение которой вам неизвестно и/или вызывает сомнения, а также с предложением оплатить комиссию/налог/страховку и т. д. для её получения, настоятельно рекомендуем не отвечать на такие сообщения и ни в коем случае не переводить деньги, т. к. это распространённый вид мошенничества.

Также мошенники могут от имени Банка России звонить, рассылать СМС-сообщения, сообщения в мессенджерах с предложением получить компенсацию за купленные ранее лекарственные средства (медицинские приборы, БАДы).

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

Для того чтобы не стать жертвами злоумышленников, будьте бдительны, всегда проверяйте информацию на достоверность и не поддавайтесь на провокации.

Во всех случаях, вызывающих подозрение, немедленно обращайтесь в правоохранительные органы!

Что делать, если с вашей банковской карты незаконно списали деньги?

– Как можно скорее позвоните в банк по номеру на обороте карты, сообщите о мошеннической операции и заблокируйте карту. Карту также можно заблокировать через приложение.

– Обратитесь в отделение банка и попросите выписку по счёту. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приёме (банк рассмотрит заявление в течение 30 дней, а если операция была международной – в течение 60 дней.)

– Обратитесь в правоохранительные органы с заявлением о хищении.

АО «Тойота Банк»
Россия, 127273, Москва
ул. Отрадная, д. 2Б, стр. 1
+7 (495) 644 1000
www.toyota-bank.ru