Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Мошенничество

2022

Содержание

Мошенничество – это обман людей с целью украсть их деньги.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенники пытаются узнать вашу секретную информацию.

Мошенники пытаются узнать ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники хотят узнать информацию о ваших банковских счетах.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Мошенники хотят узнать информацию о ваших банковских картах.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Мошенники хотят узнать ПИН-код вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль вашей банковской карты.

ПИН-код – это 4 цифры.

ПИН-код нужен, чтобы пользоваться вашей банковской картой.

ПИН-код вашей банковской карты должны знать только вы.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Мошенники хотят узнать защитный код вашей банковской карты.

Защитный код (CVV/CVC-код) – 3 цифры на оборотной стороне вашей банковской карты.

Защитный код нужен для подтверждения платежа с вашей банковской карты.

Не говорите, **не показывайте** и **не пишите** защитный код вашей банковской карты чужим людям.

Мошенники хотят узнать одноразовый пароль из СМС-сообщения от банка.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на телефон.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Мошенники обманывают людей разными способами.

Вы должны знать, как обманывают мошенники.

Тогда вы сможете защититься от мошенников.

Где мошенники могут быть опасны?

1 Мошенники могут быть опасны при использовании банкомата

Банкомат – аппарат для приёма и выдачи наличных денег.

Для использования банкомата вам нужна ваша банковская карта.

Вам нужно набрать ПИН-код вашей банковской карты.

ПИН-код – это секретный пароль вашей банковской карты.

ПИН-код — это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Другие люди **не должны** видеть ПИН-код вашей банковской карты.

Мошенники могут пытаться узнать ваш ПИН-код.

Мошенники могут:

- установить на банкомат специальное устройство
- установить видеокамеру над клавиатурой банкомата

Если мошенники получат информацию о вашей банковской карте, они могут украсть ваши деньги.

Если вы хотите снять деньги, внимательно осмотрите банкомат.

Если на банкомате есть лишние предметы, найдите другой банкомат.

Если клавиатура банкомата шатается, найдите другой банкомат.

Мошенники могут попытаться подсмотреть ваш ПИН-код.

Пользуйтесь банкоматом, когда рядом нет других людей.

Когда вы вводите ПИН-код вашей банковской карты, прикрывайте клавиатуру рукой.

Если вам трудно пользоваться банкоматом, попросите близкого человека помочь вам.

Если кто-то предлагает вам помощь у банкомата без вашей просьбы, откажитесь от помощи.

Если вы обращаетесь за помощью к чужим людям, будьте осторожны.

Не передавайте вашу банковскую карту чужим людям.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Лучше пользоваться банкоматом в офисе банка.

Если вам нужна помощь, сотрудник банка поможет вам.

2 Мошенники могут быть опасны при оплате товаров и услуг в интернете

При оплате в интернете вы вводите секретную информацию:

- номер вашей банковской карты
- срок окончания действия вашей банковской карты
- ваши имя и фамилию
- защитный код (CVV/CVC-код) вашей банковской карты

Для оплаты в интернете банки присылают вам одноразовый пароль.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на мобильный телефон.

Одноразовый пароль нужно ввести на странице оплаты.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Чтобы получать СМС-сообщения от банка, вам нужно подключить мобильный банк.

Мобильный банк – это система, которая позволяет управлять вашими деньгами в банке с помощью СМС-сообщений.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Никто **не должен** спрашивать у вас одноразовый пароль.

Одноразовый пароль спрашивают только мошенники.

СМС-сообщения из банка – это ваша секретная информация.

Никто **не должен** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

Иногда вам может позвонить сотрудник банка.

Он может спросить про последние платежи с вашей банковской карты.

Сотрудник банка **не должен** спрашивать у вас информацию вашей банковской карты.

Информацию банковской карты спрашивают только мошенники.

Если у вас спрашивают информацию вашей банковской карты, сразу завершите разговор.

3 Мошенники могут быть опасны в интернете

Чтобы узнать вашу секретную информацию, мошенники создают поддельные сайты.

Мошенники копируют сайты известных организаций.

Поддельный сайт очень похож на настоящий сайт организации.

Поддельный сайт имеет другой адрес в интернете.

Пример

Вы попали на поддельный сайт интернет-магазина.

Вы хотите оплатить покупку на этом сайте.

Вы вводите информацию вашей банковской карты.

Ваша секретная информация попадает к мошенникам.

Мошенники могут украсть ваши деньги.

Будьте внимательны!

Адреса поддельных сайтов очень похожи на адреса настоящих сайтов.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Мошенники могут прислать вам сообщение со ссылкой на поддельный сайт.

Не нажимайте на эту ссылку!

Сообщение вы можете получить:

- в телефоне
- по электронной почте
- в социальной сети

Мошенники пишут ложные сообщения.

Примеры ложных сообщений:

- ваша карта заблокирована
- с вашего банковского счёта переведены деньги
- на ваш банковский счёт зачислены деньги
- вы выиграли в лотерею
- вам нужно обновить ваши личные данные
- вам нужно подтвердить ваши личные данные

Мошенники пишут ложные сообщения, чтобы вы нажали ссылку.

Если вы нажмёте ссылку, вы попадёте на поддельный сайт.

Не нажимайте на эту ссылку!

Поддельный сайт внешне очень похож на настоящий сайт.

На поддельном сайте вас попросят ввести ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники могут украсть ваши личные данные.

Мошенники могут украсть ваши деньги.

Пример 1

Вам приходит сообщение от вашего друга.

В сообщении есть ссылка.

В сообщении говорится, что нужно нажать ссылку.

Что делать

- **не нажимайте** ссылку в сообщении
- позвоните вашему другу
- расскажите вашему другу о сообщении

Мошенники украли секретную информацию вашего друга.

Мошенники хотят украсть вашу секретную информацию.

Пример 2

Вам приходит сообщение от известного магазина.

В сообщении вам предлагают большие скидки на товары.

Вам нужно перейти на сайт по ссылке.

Чтобы получить скидку, вам нужно ввести ваши личные данные на сайте.

Что делать

- **не нажимайте** ссылку в сообщении
- найдите в интернете сайт магазина
- узнайте на этом сайте информацию о скидках

Не вводите ваши личные данные на сайте.

Известные организации никогда **не спрашивают** личные данные.

Правила безопасности:

- **не нажимайте** ссылки в неизвестных сообщениях
- **не загружайте** вложенные файлы, которые вы **не ждете**

Вложенный файл – документ, который приходит в сообщении.

Обращайте внимание на интернет-адрес в ссылке.

Обращайте внимание на адресную строку.

Интернет-адрес поддельного сайта отличается от интернет-адреса настоящего сайта.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Если вы постоянно пользуетесь сайтом, сохраните его в закладках.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Обращайте внимание на содержание сообщения.

Мошенники часто делают много ошибок.

Не звоните по телефонам из сообщения.

Найдите в интернете сайт организации.

На сайте организации вы можете найти номер телефона.

Позвоните по этому номеру телефона.

Вы сможете узнать нужную информацию.

Вы будете уверены, что вас **не обманули**.

Надёжно защитите ваши пароли.

Никому **не говорите** ваши пароли.

Запишите пароли на бумаге и храните в надёжном месте.

Никому **не передавайте** ваши пароли.

Никому **не говорите** и **не пишите** ваши личные данные.

Установите антивирус на ваши устройства.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Регулярно обновляйте программы и приложения на ваших устройствах.

4 Мошенники создают финансовые пирамиды

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Например, мошенники предлагают людям вкладывать деньги в фонд.

Мошенники обещают очень высокий доход.

Если люди вкладывают деньги в такой фонд, мошенники украдут эти деньги.

Можно вкладывать деньги только в известные финансовые организации.

Как понять, что вас обманывают?

Как понять, что вас зовут в финансовую пирамиду?

Признаки финансовой пирамиды:

- вам обещают высокий доход
- вам говорят, что нет никаких рисков
- вас просят внести деньги сразу
- вас просят внести наличные деньги
- вас просят привести друга

На финансовых пирамидах заработать нельзя.

Мошенники заберут ваши деньги.

Вы **не сможете** вернуть ваши деньги.

5 Мошенники бывают на торговых сайтах

В интернете есть торговые сайты.

На этих сайтах вы можете сами продавать и покупать товары.

На торговых сайтах вы можете встретить мошенников.

Будьте внимательны.

Мошенники могут вас обмануть.

Пример 1

Вы хотите купить товар.

Продавец товара живёт в другом городе.

Товар нужно переслать в ваш город.

Продавец требует заранее оплатить пересылку товара.

Продавец просит перевести деньги на его банковскую карту.

Что делать

- **не переводите** деньги заранее
- вы **не получите** товар
- вы потеряете деньги

Платите деньги после того, как получите товар.

Если продавец требует заранее заплатить ему деньги, **не общайтесь** с ним.

Найдите другого продавца.

Пример 2

Вы хотите что-то продать.

Покупатель хочет перевести деньги на ваш банковский счёт.

Покупатель просит у вас номер вашей банковской карты.

Покупатель просит у вас защитный код (CVV/CVC-код) вашей банковской карты.

Что делать

Защитный код банковской карты (CVV/CVC-код) – это секретный код.

Никому **не говорите** и **не пишите** защитный код вашей банковской карты.

Чтобы перевести вам деньги, покупателю нужен только номер вашей банковской карты.

Если покупатель просит вашу секретную информацию, **не общайтесь** с ним.

Пример 3

Вы разместили объявление о продаже товара.

Вы получаете СМС-сообщение с неизвестного номера.

В сообщении вы можете прочитать ложную информацию:

- ваше объявление заблокировано за нарушение правил
- есть отклик на ваше объявление
- пришлите СМС с кодом для отмены блокировки

Что делать

Не отправляйте СМС-сообщение на неизвестный номер.

Вы можете потерять много денег.

Зайдите на сайт, где вы разместили объявление.

Найдите на сайте контакты службы поддержки.

Напишите или позвоните в службу поддержки сайта.

Расскажите о сообщении, которое вы получили.

Вам скажут, что нужно делать.

6 Мошенники могут присылать электронные письма

Мошенники могут присылать вам письма на электронную почту.

Мошенники могут предлагать вам:

- много денег за помощь
- пройти опрос
- получить приз

Не верьте тем, кто предлагает вам деньги и призы.

Не отвечайте на письма от незнакомых людей.

Пример 1

Вы получаете электронное письмо.

Незнакомый человек просит вас помочь получить наследство.

Человек обещает вам за помощь много денег.

Что делать

Сразу удалите письмо.

Не верьте тем, кто предлагает вам много денег.

Если вы согласитесь помогать, вы потеряете много денег.

Пример 2

Вы получаете электронное письмо.

В письме вам предлагают пройти опрос.

Вам обещают выдать приз.

Чтобы получить приз, нужно заплатить деньги.

Что делать

Не платите деньги.

Если опрос настоящий, вам **не нужно** платить деньги.

Только мошенники просят заранее платить деньги.

7 Мошенники могут предлагать вам работу

В интернете вам предлагают устроиться на работу.

Вам предлагают большую зарплату.

Вас просят заранее оплатить услуги по устройству на работу:

- вы должны оплатить оформление документов
- вы должны оплатить пропуск на территорию организации
- вы должны купить обучающие материалы
- вы должны заплатить за обучение

Не надо платить.

Вы потеряете ваши деньги.

Вы **не получите** работу.

Помните!

Организации **не берут** деньги у будущих работников.

Только мошенники просят заплатить при устройстве на работу.

Чтобы устроиться на настоящую работу:

- вам **не нужно** платить за обучение
- вам **не нужно** покупать продукцию
- вам **не нужно** платить за трудоустройство

8 Мошенники могут говорить, что они представители банков и государственных организаций

Мошенник может представиться сотрудником вашего банка.

Мошенник может представиться сотрудником государственной организации.

Мошенники могут позвонить вам по телефону.

Мошенники могут прийти к вам домой.

Мошенники подделывают официальные документы, чтобы вы им поверили.

Будьте внимательны!

Не верьте незнакомым людям, если они звонят вам и что-то спрашивают.

Не открывайте дверь незнакомым людям!

Пример 1

Вы получаете СМС-сообщение.

В сообщении написано, что ваша банковская карта заблокирована.

Если банковская карта заблокирована, она **не работает**.

В сообщении есть номер телефона.

Вам предлагают позвонить в банк по этому номеру телефона.

Вы звоните по этому номеру.

Вам отвечают мошенники.

Мошенники спрашивают у вас информацию вашей банковской карты.

Что делать

Никому **не говорите** информацию вашей банковской карты.

Не звоните по номеру телефона в сообщении.

Позвоните в банк.

Номер телефона банка есть на вашей банковской карте.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Сотрудник банка поможет вам.

Пример 2

К вам домой приходит человек.

Человек говорит, что он социальный работник.

Он рассказывает вам про новый прибор.

Человек говорит, что этот прибор дорого стоит.

Он предлагает вам купить прибор за небольшие деньги.

Что делать

Не покупайте ничего у чужих людей, которые пришли к вам домой.

Вы потеряете ваши деньги.

Не пускайте чужих людей в дом, если вы их **не приглашали**.

Чужие люди могут обмануть вас.

Чужие люди могут украсть у вас деньги и вещи.

Правила безопасности

Когда вы пользуетесь банковской картой:

- **не оставляйте** вашу банковскую карту без присмотра
- **не передавайте** никому вашу банковскую карту
- никому **не говорите**, **не показывайте** и **не пишите** ПИН-код вашей банковской карты
- никому **не сообщайте** информацию, которую вы получили от банка

Сотрудник банка **не имеет права** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

При любых проблемах с вашей банковской картой срочно звоните в банк.

Телефон банка есть на обороте вашей банковской карты.

Телефон банка вы можете найти на сайте вашего банка.

Используйте банкоматы в безопасных местах.

Не открывайте файлы и ссылки из незнакомых источников.

Установите антивирус на ваших устройствах.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Когда вы пользуетесь интернетом, **не пользуйтесь** публичным Wi-Fi.

Wi-Fi – это беспроводной интернет.

Публичный Wi-Fi – это беспроводной интернет в общественном месте.

Пользуйтесь только безопасными сайтами.

Адрес безопасного сайта начинается так:

https://

В адресной строке безопасного сайта вы увидите значок в виде замка:

Знак безопасного сайта

Загружайте приложения для смартфона только с официальных сайтов.

Приложение с другого сайта может содержать вредные программы.

Будьте внимательны, когда загружаете банковские приложения на смартфон.

Обращайте внимание, кто создал банковское приложение.

Официальные банковские приложения создаёт сам банк.

Не загружайте приложения от других организаций.

Оплачивайте покупки только на сайтах с защищённым соединением.

На этих сайтах должен быть значок платёжной системы вашей банковской карты.

Если на сайте нужно ввести ваши личные данные, будьте осторожны.

Если вам звонят незнакомые люди.

Будьте внимательны! Проверяйте информацию.

Позвоните в организацию по официальному номеру телефона.

Номер телефона вы можете найти на сайте организации.

Если вам сообщили о блокировке банковской карты, позвоните в ваш банк.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Телефон банка есть на обратной стороне вашей банковской карты.

Телефон банка вы можете найти на сайте банка.

Адрес сайта банка вы можете найти на сайте Банка России:
http://cbr.ru/banking_sector/credit/FullCoList

Никогда **не спешите** платить деньги.

Спокойно подумайте.

Посоветуйтесь с близким человеком.

Если вас обманули, сразу обратитесь в полицию.

Словарь

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Банковская карта позволяет вам пользоваться деньгами с вашего банковского счёта.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Банкомат – аппарат для приёма и выдачи наличных денег.

Вложенный файл – документ, который приходит в сообщении.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Защитный код (CVV/CVC-код) — 3 цифры на оборотной стороне вашей банковской карты.

Личные данные – это информация из ваших документов.

Мобильный банк – это способ управления вашим банковским счетом через СМС-сообщения.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенничество – обман людей с целью украсть их деньги.

Одноразовый пароль вы можете использовать только один раз.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль банковской карты.

ПИН-код нужен, чтобы пользоваться банковской картой.

ПИН-код – это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Поддельный сайт очень похож на настоящий сайт организации, но имеет другой адрес в интернете.

Поддельные сайты создают мошенники.

Публичный Wi-Fi – беспроводной интернет в общественном месте.

СМС-сообщение (СМС) – это текстовое сообщение в мобильном телефоне.

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Wi-Fi – это беспроводной интернет.

Запомните!

Не бойтесь просить помощи, если вы в чём-то не уверены.

Кто может помочь вам понять финансовые вопросы?

Куда вы можете обратиться за дополнительной информацией?

Вы можете получить помощь и узнать ответы на ваши вопросы здесь:

- **Ваша семья и ваши друзья**
- **Ваш банк**
  Вы можете написать свои вопросы на сайте банка.
  Вы можете позвонить в ваш банк по телефону. Контактные данные вы можете найти на сайте банка в интернете.
  Вы можете прийти в офис банка и задать вопросы сотруднику банка.

Банк России

Вы можете задать вопрос в чате мобильного приложения «ЦБ онлайн».

Вы можете позвонить по телефону:
8-800-300-30-00

АНО «Наш Солнечный Мир»

Вы можете прислать вопросы по электронной почте: info@solnechnymir.ru

Сайт «Финансовая культура»:
www.fincult.info/feedback

Вы можете найти ответ на ваш вопрос
на этом сайте.
Вы можете написать вопрос на этом сайте.