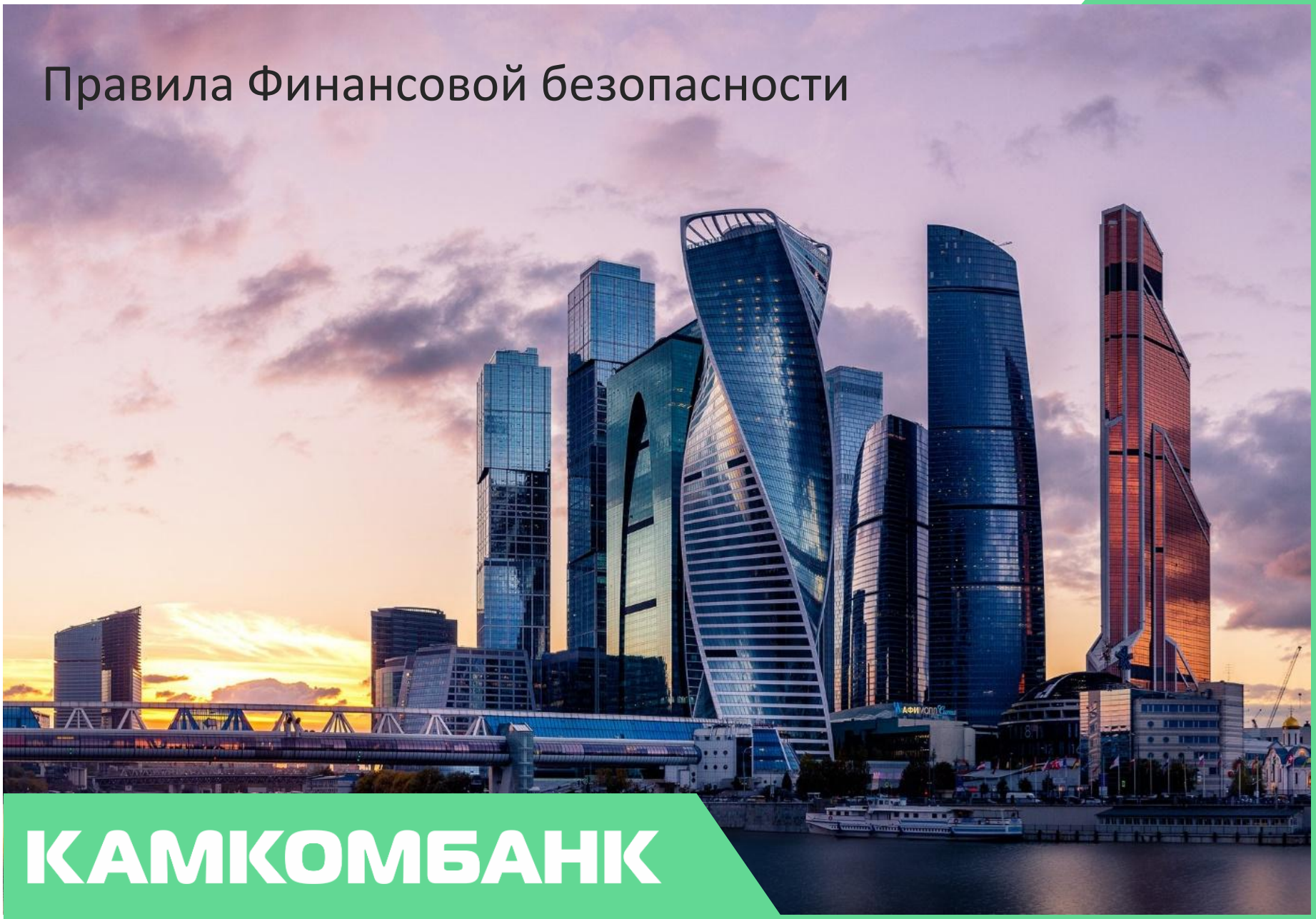
Правила Финансовой безопасности



КАМКОМБАНК

WWW.KAMKOMBANK.RU

Меры безопасности при работе на сайте ООО «Камкомбанк»

1. В интернете могут быть сайты, которые внешне маскируются под систему Камкомбанк. Их основная цель – попытка перехвата личных данных клиентов банка. Осуществляйте работу только на официальном сайте https://www.kamkombank.ru/.

2. Не оставляйте без присмотра компьютер, пока происходит сеанс связи с банком.

3. Используйте на своих компьютерах антивирусные программы и регулярно обновляйте их.

4. Обязательно смените пароль в случае, если он стал известен посторонним лицам.

5. Не используйте сохранение паролей к сайтам в браузере, т.к. сохраненные данные могут стать легкой добычей злоумышленников при проведении атаки на браузер.

6. Не храните на серверах электронной почты (в особенности, на бесплатных ресурсах) письма, содержащие конфиденциальную информацию, в частности, переписку с банком. Данная информация может стать добычей для злоумышленников и быть использована ими в личных целях.

7. Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам банка обо всех подозрительных или несанкционированных операциях.

8. Никогда не отвечайте на письма от имени системы Камкомбанк, в которых предлагается зайти на сайт, не принадлежащий домену www.kamkombank.ru или на нем скачать программу для установки. ООО «Камкомбанк» не осуществляет рассылку подобных электронных писем. Пожалуйста немедленно сообщите о подобном факте в банк по номеру телефона, указанному на оборотной стороне банковской карты либо по телефону 8-800-2000-438 (звонок по России бесплатный)

Меры безопасности при использовании мобильного приложения

1. Не устанавливайте код безопасности, который состоит из одинаковых цифр.

2. Будьте внимательны — не оставляйте свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг. Клиент несет личную ответственность за нарушение правил хранения носителей средств авторизации и разглашение пароля доступа к системе, в случае если данные операции были проведены злоумышленниками посредством мобильного устройства клиента.

3. Риск мошенничества уменьшается при использовании в мобильном приложении двухфакторной аутентификации (ввод логина/пароля и одноразового пароля для подтверждения входа/платежа).

4. Не храните код безопасности CVC2 виртуальной карты на своем телефоне.

5. При потере мобильного телефона с подключенной услугой «SMS-Информатор», установленным мобильным приложением вам следует немедленно обратиться к оператору сотовой связи для блокировки SIM-карты и по номеру телефона, указанному на оборотной стороне банковской карты либо по номеру 8-800-2000-438 (звонок по России бесплатный).

6. При установке на телефон дополнительных программ обращайте внимание на разрешения, которые запрашивает программа. Если программе требуются излишние полномочия, это повод проявить настороженность, например: доступ и отправка SMS, доступ к сети Интернет.

7. Установите пароль для доступа на ваш телефон.

8. Установите и своевременно обновляйте антивирусное ПО на вашем телефоне.

9. Не храните пароль для доступа в приложении на своем телефоне.

10. Никому не сообщайте свой пароль.

Меры безопасности при пользовании банковскими картами

Если вы потеряли карту банка

Немедленно сообщите об утере/хищении карты в банк для её блокировки. Эта мера предотвратит несанкционированное использование карты сторонними лицами.

Совершение операций в интернете с использованием карты банка

1. Рекомендуем вам использовать для оплаты в интернете отдельную карту с подключенной услугой «SMS-Информатор» с минимально необходимым остатком на карте. Нежелательно использовать в интернете карту, на которую приходят регулярные начисления, например, заработная плата или пенсия.

2. При расчетах в интернете самостоятельно оценивайте надежность сайта фирмы-продавца, на котором вы будете указывать реквизиты вашей карты. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

3. Соблюдайте конфиденциальность персональных данных/информации о карте, для этого:

   - В случае совершения операции покупки с использованием чужого компьютера удаляйте все персональные данные/данные о карте. После завершения всех операций убедитесь, что конфиденциальная информация не сохранилась;
   - Не отвечайте на электронные письма, в которых у вас просят предоставить персональные данные и данные карт. Не следуйте по ссылкам, указанным в подобных письмах, так как они могут вести на фишинговые сайты-двойники;
   - Не используйте ПИН-код при оплате товаров и услуг через интернет.

Меры безопасности при пользовании банковскими картами

4. Оплачивая товары/услуги в интернете при помощи карты, обязательно сохраняйте контактную информацию (телефон, интернет адрес) организации, предоставившей товары/услуги.

5. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в интернете использовать отдельную банковскую карту/виртуальную карту с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

ВНИМАНИЕ! Банк предупреждает о повышенном риске при совершении операций в сети Интернет! При размещении в интернете своих персональных данных/реквизитов виртуальной карты учитывайте возможность утечки информации и использования её мошенниками!

Меры безопасности при разговоре по телефону о продуктах и услугах банка

1. В последнее время участились случаи мошенничества с банковскими картами после подачи клиентами-держателями карт объявлений о продаже какого-либо имущества, например, на сайте www.avito.ru. Мошенник действуют следующим образом: откликается на объявление о продаже, сообщает, что готов перевести предоплату за продаваемый предмет, для чего запрашивает данные карты (номер карты, дату истечения срока действия и т. д.). Вас также могут попросить сообщить отправленный на ваш телефон код. Далее вместо зачисления на карту мошенник списывает денежные средства с вашей карты. Будьте бдительны! Для зачисления на карту достаточно сообщить только номер карты. Не предоставляйте реквизиты своих банковских карт третьим лицам, не сообщайте одноразовые пароли, не совершайте никаких действий в банкомате по инструкции незнакомых. При обнаружении операций, которые вы не совершали, незамедлительно обратитесь в банк по номеру телефона, указанному на оборотной стороне банковской карты либо по номеру 8-800-2000-438 для блокировки карты.
2. Известны случаи, когда на телефон клиента приходит сообщение якобы от банка о блокировке карты с указанием контактного номера телефона, по которому нужно перезвонить для разблокировки карты. Затем, когда держатель карты перезванивает по указанному номеру, его просят сообщить данные карты или подойти к ближайшему банкомату и перевести средства с карты на определенный номер мобильного телефона. Далее держатель карты неосознанно под диктовку неизвестного голоса в телефоне переводит свои средства в пользу мошенников.

ПОМНИТЕ! При получении подобных СМС-сообщений необходимо звонить в банк только по номеру, указанному на оборотной стороне банковской карты для уточнения деталей о блокировке карты.

Меры безопасности при посещения офиса банка

- При обслуживании в банке старайтесь не называть громко сумму и вид операции;
- Пересчитывайте деньги при сотруднике банка;
- складывайте деньги и документы в сумку/кошелек при сотруднике банка;
- Не называйте громко свои личные данные (серию и номер паспорта, номер СНИЛС, номер телефона, адреса регистрации/проживания);
- Обязательно сообщите сотруднику банка, если:
  - Если вы пришли в офис банка не добровольно, а под психологическим влиянием иного лица;
  - Если при входе в банк вы заметили подозрительного человека (агрессивный, психологически неуравновешенный, в алкогольном опьянении и т.п.).

Меры безопасности от кредитных мошенников

Чтобы эффективно защищаться от мошенников, важно разобраться в основных методах, которые они используют для получения доступа к вашим кредитным данным.
Один из наиболее распространенных способов мошенничества с кредитами — это подделка личных данных. Преступники могут подать заявку на кредит от вашего имени, узнав такие персональные сведения, такие как имя, адрес, номер СНИЛС, дата рождения.

Другой вариант — фишинг. Это метод мошенничества, когда злоумышленники создают поддельные электронные письма, веб-сайты или сообщения с целью обмануть вас и выманить личные данные. Такие письма и сообщения могут выглядеть абсолютно правдоподобно и часто содержат просьбы предоставить логин, пароль, номера банковских счетов или другую конфиденциальную информацию. Понятно, что, завладев этими данными, преступники используют их совсем для собственной наживы.

Как повысить безопасность личных данных

Охрана личной информации является первоочередной задачей для каждого пользователя банковскими услугами. Вот какие шаги можно предпринять для этого:

Позаботьтесь о создании надежных паролей
Это один из важнейших шагов для защиты ваших финансов. Используйте уникальные пароли для каждого аккаунта, избегая очевидных комбинаций типа «123456» или дату рождения. Ваши пароли должны содержать не только буквы (прописные и строчные), но и цифры и специальные символы.

Осторожнее с личными данными в соцсетях
Мошенники могут использовать информацию, опубликованную вами в социальных сетях, для выявления личных данных. Будьте внимательны к тому, что вы публикуете о себе, и избегайте раскрытия такой информации, как дата рождения, адрес, номера телефонов и др.

Подготовьтесь к возможным атакам аферистов
Следует точно знать, как действовать, если вы столкнетесь с мошенничеством. Сохраните номера телефонов банка для блокировки банковских карт и другую полезную информацию на тот случай, если понадобится срочная помощь со стороны вашего финансового учреждения.

Меры безопасности от кредитных мошенников

Защита от мошенников по кредитам, использующих фишинговые схемы

Фишинг являются популярными методами мошенников, которые пытаются выманить ценные данные. Как успешно предотвратить мошенничество? Берите следующие советы на вооружение.

- **Научитесь распознавать поддельные электронные письма и веб-сайты.**
Они могут выглядеть почти так же, как официальные. Обратите внимание на некорректную грамматику, орфографические ошибки или странные домены электронных адресов. Не нажимайте на подозрительные ссылки и не отвечайте на письма, в которых просят предоставить конфиденциальную информацию.

- **Игнорируйте подозрительные запросы** *на предоставление паролей, номеров банковских счетов, номеров СНИЛС или другой личной информации. Они могут поступать через электронную почту, телефон или сообщения. Любой похожий запрос должен вызвать у вас подозрение.*

- **Проверяйте правомерность запросов на предоставление информации.** *В случае сомнений обращайтесь напрямую в банк. Никогда не используйте контакты, предоставленные в подозрительных письмах или сообщениях.*

- **Проявляйте бдительность при общении по телефону.** *Мошенники нередко звонят и выдают себя за сотрудников банка, просят подтвердить личные данные. Будьте внимательны и убедитесь, что разговариваете с официальным представителем банка. В случае сомнений отложите звонок и перезвоните сами по официальному номеру банка.*

- **Постоянно обновляйте свои знания** *о современных мошеннических схемах и методах защиты. Знакомьтесь с информацией от банков и экспертов в сфере кибербезопасности.*

- **Правильно реагируйте на подозрительные ситуации.** *Если вы столкнулись с непонятной ситуацией, не стоит паниковать. Сохраните все доказательства, такие как электронные письма или номера телефонов. Если ситуация оказалась мошенничеством, немедленно сообщите об этом в банк и в правоохранительные органы.*

Сохранение в безопасности ваших личных данных — ключ для предотвращения мошенничества с кредитами

Меры безопасности от кредитных мошенников

Что нужно знать при заполнении заявок на кредит

Заполнение заявок на кредит может быть источником рисков, особенно если злоумышленники получат доступ к вашей конфиденциальной информации. Вот несколько советов, как быть более осторожными и повысить защиту от мошенников.

- **Проверяйте надежность кредитора.** Прежде чем подавать заявку на кредит, проведите тщательный анализ кредитора. Убедитесь, что это лицензированное и надежное финансовое учреждение. Изучите рейтинги и отзывы других клиентов. Будьте осторожны с предложениями, которые кажутся слишком заманчивыми.

- **Проявляйте осторожность при предоставлении данных.** Заполняя заявки на кредит, предоставляйте только необходимую информацию. Будьте особенно осторожны с личными данными, такими как номер СНИЛС, финансовая информация и пароли. Надежные банки обычно не требуют предоставлять слишком много личных данных в начальной заявке.

- **Следите за документами, которые вы предоставляете при заполнении заявок на кредит.** Убедитесь, что документы хранятся в надежных местах и не могут попасть в руки посторонних.

- **Избегайте заполнения заявок на кредит на общедоступных компьютерах или в сетях Wi-Fi**, которые недостаточно защищены. Используйте для этого личное устройство и надежное интернет-подключение.

- **Своевременно удаляйте информацию.** Если вы решили отказаться от заполнения заявки или изменить свое решение, сотрите всю введенную информацию перед закрытием окна браузера. Не оставляйте конфиденциальные данные без удаления.

Меры безопасности от кредитных мошенников

Что делать, чтобы не нарваться на мошенников по кредиту

1. Регулярно проверяйте свою кредитную историю. Дважды в год это можно сделать бесплатно. Это позволит вам выявить любые несанкционированные запросы или активности, которые могли бы указывать на попытки мошенничества.
2. Мониторьте операции на своих банковских счетах и кредитных картах. Если вы обнаружите непонятные или несанкционированные транзакции, немедленно свяжитесь с банком или кредитором для выяснения ситуации.
3. Если вы столкнулись с мошенничеством или обнаружили подозрительную активность, сразу же свяжитесь с банком, чтобы получить инструкцию по дальнейшим действиям.
4. Сохраняйте копии всех документов и электронных писем, связанных с мошенничеством или подозрительной активностью. Эти доказательства могут быть полезными при разборе ситуации в банке.

Совет! Постоянно обновляйте свои знания о новых схемах мошенничества и методах защиты. Будьте бдительны при совершении финансовых операций и не стесняйтесь обращаться за помощью в банк, если у вас возникли подозрения.

Подводим итоги

Выделим ключевые шаги, которые помогут вам эффективно обезопасить свои финансы и повысить защиту от оформления кредита мошенниками.

- Регулярно обновляйте программное обеспечение на ваших устройствах, используйте антивирусные программы и ставьте сложные пароли. Не делитесь своими паролями или личными данными с посторонними.
- Постоянно пополняйте копилку своих знаний о схемах мошенничества и методах защиты. Читайте статьи, просматривайте информацию от банков и из других официальных источников.
- Время от времени проверяйте свою кредитную историю на наличие подозрительной активности. Это позволит вам быстро выявить мошенничество и принять меры.
- Заполняя заявки на кредит, будьте внимательны к предоставляемой информации. Не давайте лишних данных и следите за сохранностью документов.
- Если вы столкнулись с мошенничеством или подозрительной активностью, немедленно принимайте меры. Для этого свяжитесь с банком и обратитесь в полицию.
- При общении с банками, кредиторами или организациями доверяйте только официальным контактам. Не предоставляйте личные данные или средства через неофициальные каналы.
- Сохраняйте копии всех документов и электронных писем, связанных с мошенничеством или подозрительной активностью.

Используйте безопасные способы оформления кредита — в отделении банка или на официальном сайте. Например, прямо сейчас вы можете сделать запрос на кредит наличными на выгодных условиях с услугой «Гарантированная ставка». Листайте вниз, чтобы оставить онлайн-заявку и узнать подробности.

8-800-2000-438

Центральный офис.

423807, г. Набережные Челны,
ул. Гидростроителей, 21
Камский Коммерческий Банк

WWW.KAMKOMBANK.RU