МИНИСТЕРСТВО ТОРГОВЛИ И УСЛУГ
РЕСПУБЛИКИ БАШКОРТОСТАН

ПАМЯТКА ПОТРЕБИТЕЛЮ

ИНФОРМАЦИОННАЯ И ФИНАНСОВАЯ БЕЗОПАСНОСТЬ ВОПРОСЫ И ОТВЕТЫ

В XXI веке одним из важных признаков грамотного человека становится знание правил кибербезопасности и умение распоряжаться финансами в цифровом мире.

Усилия мошенников в основном направлены на получение платежной информации: номеров и CVV-кодов кредитных карт, логинов и паролей к интернет-банкингу. Банки и платежные системы постоянно совершенствуют системы безопасности, чтобы защитить деньги и персональные данные своих клиентов. Но техника бессильна, если сами клиенты будут забывать о мерах предосторожности.

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

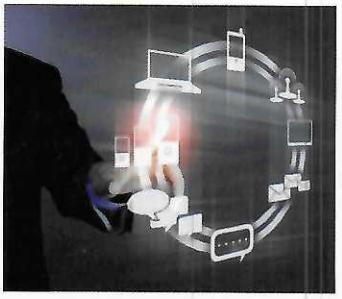
Немедленно прервите разговор, несмотря на угрозы и давление. Чтобы войти в доверие, злоумышленники могут обращаться к вам по имени и отчеству. Не поддавайтесь на уловки. Самостоятельно позвоните в банк по номеру телефона, указанному на его официальном сайте или на обратной стороне карты.

Позвонили и предложили перевести деньги на специальный счет в центробанке. Что делать?

Это наиболее распространенная мошенническая схема. Не существует «специальных», «безопасных», «защищенных» или каких-то других счетов, на которые граждане должны переводить деньги в адрес Центрального банка. Злоумышленники упоминают якобы специальный счет в Центробанке, чтобы усыпить бдительность человека. Счет, реквизиты которого называют мошенники, принадлежит им. Не совершайте никаких действий по своему счету, положите трубку.

Если у вас остались какие-то 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 человека пытаются выяснить данные карты, пароли или коды из СМС, либо провоцируют самостоятельно перевести деньги. Поэтому важно помнить: никогда не сообщайте данные своей карты, пароли из СМС, не переводите деньги на счет по просьбе неизвестного абонента, кем бы он не представлялся. Также никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС, а еще лучше вообще не переходите на сайты по ссылкам из подозрительных писем.

Приходит сообщение о необходимости подтвердить покупку, которую вы не совершали. Что делать?

Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается 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 счета средства или подписать вас на ненужный платный сервис. Если вам придет сообщение о необходимости подтвердить покупку — игнорируйте его.

Как узнать фишинговый сайт и как не стать жертвой фишинга?

В Интернете множество фишинговых сайтов — это подделки под сайты настоящих финансовых (банков, страховых компаний и др.) или любых других организаций, которые сильно похожи на официальный сайт компании. Цель фишинговых сайтов — выманить личные и финансовые данные, которые нужны мошенникам для кражи денег.

Как правило, жертвы попадают на фишинговые сайты через ссылки, которые приходят в письмах или СМС. Не переходите по ссылкам из подозрительных сообщений. Пользуйтесь только проверенными ресурсами.

Какую информацию о своей банковской карте ни в коем случае нельзя сообщать посторонним людям?

Если кто-либо запрашивает у вас номер карты, срок действия, код проверки подлинности карты (три цифры на обратной стороне — CVV или CVC), ПИН-код, а также код из СМС для подтверждения платежей и переводов — это мошенник. Ни в коем случае не сообщайте эти данные в разговоре с незнакомым человеком.

Никогда и никому не сообщайте информацию о ПИН-коде: ее не знает и не должен знать даже банк, в котором обслуживаетесь.

На чем играют мошенники, чтобы выманить у вас нужную им информацию?

Собеседник активно использует ваше чувство страха (ваша карта заблокирована, вы можете потерять деньги, данные украдены и т.д.), давит на жажду наживы (пройдите опрос и получите вознаграждение, получите компенсацию, выплату, очень выгодные условия по кредиту или вкладу и т.д.). При этом требуют срочно принять решение и совершить некоторые действия: сообщить персональные данные, проделать определенные манипуляции с банковской картой. В противном случае вам угрожают потерей денег или возможности получить их.

Имейте в виду: даже если банк действительно зафиксировал попытку несанкционированной операции с вашего счета, он имеет право приостановить эту операцию на срок до двух суток, поэтому настоящий представитель кредитной организации не будет торопить вас принимать решение. Также вас всегда должны настораживать предложения получить легкие деньги, очень выгодные условия по кредитам или депозитам.

Источник информации: официальный сайт СБП ЦБ РФ: https://cbr.ru/faq/information_security/

При необходимости личного приема или для составления проекта досудебной претензии потребители могут обратиться в Минторг РБ по адресу:
450008, г. Уфа, ул. Цюрупы, 13, кабинет 703
с 9.00 до 18.00 по будням, перерыв с 13.00 до 14.00

Телефон «горячей линии»
8 (347) 218-09-78

Уфа-2024

Посетите раздел «Защита прав потребителей» сайта Минторга РБ, где размещена актуальная информация для потребителей.