Будьте осторожны и внимательны!

Операции с использованием банковских карт уже давно стали неотъемлемой частью нашей повседневной жизни. Карты упрощают процесс оплаты товаров и услуг, а также помогают защитить денежные средства, ведь украденная карта бесполезна, если не знать её ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от соблюдения держателем карты правил её использования: небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана.

Стать жертвой мошенников очень легко, а способ обезопасить себя и свои деньги только один: знать и соблюдать простые правила безопасного использования банковских карт.

Внимательно ознакомьтесь с содержанием этой памятки и следуйте данным рекомендациям – они защитят вас от действий мошенников и сберегут ваши средства!

Банк России
Центральный банк Российской Федерации

Отделение по Хабаровскому краю
Дальневосточного главного управления
Центрального банка Российской Федерации

www.cbr.ru

Краткая памятка для держателей банковских карт

Правила безопасного использования банковских карт

ПИН-КОД — КЛЮЧ К ВАШИМ ДЕНЬГАМ

Никогда и никому не сообщайте ПИН-код вашей карты! Относитесь к нему, как к ключу от сейфа с вашими средствами: безопаснее всего запомнить ПИН-код. Нельзя хранить ПИН-код вместе с картой и тем более записывать ПИН-код на неё – в этом случае вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или потери.

ВАША КАРТА – ТОЛЬКО ВАША

Не позволяйте никому использовать вашу пластиковую карту – это то же самое, что отдать свой кошелёк в чужие руки.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если в телефонном разговоре, по SMS или в письме, полученном по электронной почте (в том числе из банка), вас под различными предлогами просят сообщить реквизиты карты и её ПИН-код – ни в коем случае не делайте этого.
Не отвечайте на сомнительные сообщения и электронные письма, не перезванивайте по указанным в таких сообщениях телефонам и не переходите по ссылкам на веб-сайты.

ПОМНИТЕ! ХРАНЕНИЕ ПИН-КОДА В ТАЙНЕ – ЭТО ВАША ОТВЕТСТВЕННОСТЬ И ОБЯЗАННОСТЬ

ОБРАЩАЙТЕ ВНИМАНИЕ НА ОБОРУДОВАНИЕ БАНКОМАТА

Картоприемник и клавиатура банкомата не должны быть оборудованы какими-либо дополнительными устройствами. Если банкомат выглядит подозрительно – не используйте его и сообщите об этом в банк по указанному на банкомате телефону.

ОБРАЩАЙТЕ ВНИМАНИЕ НА РАБОТУ БАНКОМАТА

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования: велика вероятность того, что он перепрограммирован мошенниками.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах, оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. По всем возникающим вопросам обращайтесь ТОЛЬКО в обслуживающий банк, телефон которого указан на обороте вашей карты.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с вашей картой должны происходить в вашем присутствии.
В противном случае мошенники могут получить реквизиты вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления дубликата.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ

Если вы потеряли карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Чтобы не терять драгоценные минуты, держите телефон банка в записной книжке или в списке контактов вашего мобильного телефона.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.
Реквизиты и любая прочая информация о том, сколько средств вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

РЕГУЛЯРНО ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВАШИХ ПЕРСОНАЛЬНЫХ УСТРОЙСТВ