Цифровое мошенничество

Появление компьютеров, сотовой связи, различных мобильных приложений, позволяющих дистанционно распоряжаться владельцам их денежными средствами, хранящимися на счетах – нового финансового инструмента – банковских карт, а также их дальнейшее развитие и масштабное применение во всем мире способствовали активному внедрению методов дистанционного банковского обслуживания для физических и юридических лиц.

Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний. Одновременно с развитием таких устройств появляются новые виды обмана, позволяющие злоумышленникам присвоить денежные средства граждан, что приводит к увеличению количества обращений граждан в правоохранительные органы, в том числе и в органы прокуратуры за помощью.

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Банковская карта – это пластиковая карта для совершения платежей и доступа к средствам, хранящимся на счёте, не требующая для этого Вашего присутствия в банке. Но за счет простоты использования которых, у мошенников появляется множество способов для обмана.

КАК ЭТО РАБОТАЕТ:

Вы приобретаете товар в интернет-магазине, но затрудняетесь оплатить товар онлайн (не выходя из дома). Тогда продавец предлагает и отправляет Вам ссылку, перейдя по которой достаточно заполнить данные банковской карты и оплатить.

ЧТО ПРОИСХОДИТ НА САМОМ ДЕЛЕ:

Как только Вы переходите по ссылке и заполняете данные банковской карты, деньги будут сняты с Вашего счета. Но так как Вы попались на «удочку» злоумышленников, товар Вы не получите

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Ни при каких обстоятельствах не сообщайте никому данные банковской карты! Никогда не переходите по ссылкам, направленным сторонними приложениями (не официальным приложением интернет-магазина) для оплаты! Ни один сотрудник банка не в праве требовать трехзначный код на обороте Вашей карты!

В случае, если Вы уже перешли по ссылке, ни в коем случае не заполняйте данные вашей банковской карты! Позвоните в банк по номеру, указанному на пластиковой карте или в официальном приложении банка.

ОБЩИЕ РЕКОМЕНДАЦИИ ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ

В последнее время увеличивается число случаев мошенничества с пластиковыми банковскими картами. Чтобы не стать жертвой мошенников, следует соблюдать следующие правила безопасности:

1. Никогда и никому не сообщайте ПИН-код Вашей карты.

2. Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту в случае ее утери или если ее похитят.
3. Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.
4. Не переходите по ссылкам, указанных в сообщениях, на электронной почте, в различных мессенджерах. Даже если указанные ссылки отправил вам продавец товара, который вы решили приобрести в интернет-магазине.
5. Если Вы потеряли карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите номер телефона банка в записной книжке или в списке контактов Вашего мобильного телефона.
6. Используя в банкоматах пластиковые карты, следите, чтобы рядом не было посторонних людей.
7. Набирая ПИН-код, прикрывайте клавиатуру рукой.
8. Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.
9. В случае некорректной работы банкомата, если он самопроизвольно перезагружается, – откажитесь от его использования.
10. Никогда не прибегайте к помощи либо советам посторонних людей при проведении операций с банковской картой в банкоматах. Свяжитесь с со службой поддержки Вашего банка – они обязаны проконсультировать Вас по всем интересующим вопросам.

Указанный в данной памятке способ обмана граждан и хищения денег является самым распространенными в настоящее время.

Расследование преступлений данной категории осложняется постоянным изменением и усовершенствованием злоумышленниками способов обмана.

БУДЬТЕ БДИТЕЛЬНЫ!