Мошенники в киберпространстве и как им противостоять!

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя Ваши эмоции.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;

2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;

3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.

Помните! Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.

Обращаем Ваше внимание, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.

Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в Банк по номеру, указанному на Вашей банковской карте.

Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);

2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по указанному на банковской карте или официальном сайте номерам;

3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка — это повод уточнить ее достоверность и перезвонить в Банк;

4. Работники Банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему дистанционного банковского обслуживания (Интернет-банкинг, М-банкинг и другие). В такой ситуации немедленно прервите разговор и свяжитесь с Банком;

5. Никому и никогда не сообщайте данные своей карточки и всегда держите ее в поле зрения при совершении платежей;

6. Обязательно подключите 3D-secure и смс-оповещение;

7. Используйте только официальный сайт Банка для входа в систему Интернет-банкинга или официальное мобильное приложение;

8. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания, а также для подтверждения платежей;

9. В случае выявления действий по карточке, которые вами не совершались, необходимо оперативно обратится в Банк или самостоятельно заблокировать карточку в системе дистанционного банковского обслуживания.