«Осторожно - мошенники! Распространенные схемы дистанционных мошенничеств на территории Костромской области».

Что же такое - дистанционное преступление?

Оно включает в себя преступления, совершённые посредством сотовой связи и сети Интернет, которые осуществлены бесконтактным способом. То есть преступник, и жертва зачастую находятся на огромных расстояниях друг от друга.

Двумя самыми лидирующими схемами, которые часто используются мошенниками, являются: **подозрительные транзакции** (под видом сотрудника банка); **покупка-продажа товаров через сеть «Интернет»** (Авито, юла, и др.).

И начнем с самой популярной схемы, которая занимает первое место по распространенности «Под предлогом подозрительных транзакций». Расскажу, как происходит разговор между мошенником и его жертвой, а также самые популярные предлоги под видом, которых у вас похищают ваши денежные средства.

Преступник представляется сотрудником банка, в своей речи употребляет банковские термины, говорит убедительно, речь четкая, он сообщает о той проблеме, которая якобы возникла с вашей банковской картой, с вашими денежными средствами. блокировке карты, либо же сообщает о том, что на вас был оформлен кредит неизвестным вам человеком, и далее мошенник просит выполнить определённый порядок действий, тем самым он как будто помогает вам сохранить денежные средства.

В данной схеме есть несколько предлогов, которые использует мошенник:

1. Под предлогом аннулирования заявки на кредит.
2. Под предлогом подозрительных операций на вашем счете(кто-то пытается совершить покупку)
3. Под предлогом обналичивания бонусов от банка
4. Под предлогом блокировки банковской карты
5. Под предлогом установки приложения и другие.

Мошенники координируют действия жертвы по телефону: предлагают пройти к банкомату, говорят о необходимости вставить в него карту и под их диктовку провести несколько операций, или мошенник говорит зайти в мобильные приложение, через которые вы управляйте своими денежными средствами, где также выполнить ряд операций, которые вам диктует мошенник.

В результате потерпевший, ничего не подозревая, переводит денежные средства со своей банковской карты на абонентские номера или счета мошенников, либо же может оформить на себя кредит.

Аннулирование заявки на кредит:

- Представляется сотрудником службы безопасности банка (обращается к Вам по имени, может назвать аще место жительства);
- Сообщает о том, что неизвестное лицо оформило онлайн-заявку на кредит на определенную сумму;
- Уточняет информацию о том, подтверждайте ли Вы эту заявку;
- Доводит информацию о том, что это орудуют мошенники, которые пытаются похитить Ваши денежные средства;
- Далее «сотрудник банка» координирует действия своей жертвы по телефону, в результате чего похищает денежные средства.

Мошенники всяческими способами пытаются узнать все данные вашей банковской карты, в том числе и коды, которые вам приходят в смс-сообщении, чтобы похитить денежные средства!

Также мошенники могут представляться сотрудниками правоохранительных органов, которые якобы взаимодействуют с сотрудниками банка! (для этого отправляют фотографии удостоверений и используют подмену номера).

СОВЕТЫ:

- Не передавать данные своей банковской карты никому, не вводить их на подозрительных сайтах!
- Помнить, что реальные сотрудники банков никогда не спрашивают и не уточняют номера банковских карт и счетов, тем более – ПИН и CVV-коды!
- Если вас об этом просят, требуют немедленного ответа, пугая тем, что иначе вы лишитесь своих денег, – значит, вам звонят мошенники!
- Обращайте внимание на то, с каких абонентских номеров вам происходит звонок, обычно мошенники используют номера с кодом города (+7-(**495)…. и +7-(499)…**)!
- Мошенники могут позвонить с любого абонентского номера, так как они используют подмену номеров! Поэтому вызовы от мошенников могут поступить, как с официальных номеров банка, а также отделов полиции!
- Не торопитесь следовать инструкциям и отвечать на запрос!
- Проверьте информацию, позвонив в контактный центр банка!
- Пользуйтесь только теми операциями, в которых вы разбираетесь и уверены!
- Прежде чем что-либо предпринять, посоветуйтесь с сотрудниками банка, узнайте о безопасности операции, посмотрите в Интернете!

2.Вторым по популярности приёмом является размещение на интернет-сайтах объявлений якобы о продаже/покупке товаров. (либо же псевдо-продавец прикладывает видео товара, фото, фото своего паспорта, фото квитанций об отправке, не надо на это вестись, все это можно сделать с помощью программ-фотошоп; а сами же фото и видео товаров они берут с объявлений например с другой страны. Предлагают перейти на общение в мессенджерах.

Иногда мошенники сами звонят или пишут по объявлению о продаже товара. Представляются возможными покупателями, предлагают внести предоплату, говорят, через популярный интернет сайт, предлагают осуществить оплату за товар посредством «безопасной сделки» (+Яндекс.Доставка). Покупатель присылает ссылку якобы интернет-сайта через который осуществляется продажа, покупка товара. (то есть данная ссылка является зеркальной, идентичной, оформлена под авито)» После покупатель предлагает продавцу перейти по ссылке, ввести свои данные и данные карты, чтобы получить предоплату, после введенных данных денежные средства снимаются.

СОВЕТЫ:

- Обратить внимание, на населенный пункт, который указан в объявлении и с какого номера с вами ведёт продавец/покупатель переписку. (Пример: в объявлении указан г. Киров, а абонентский номер принадлежит к Московской области);
- Обратитесь к интернету, проверьте абонентский номер или интернет-сайт, возможно, по этим данным в сети «Интернет» будет иметься полезная информация или отзывы других людей;
- предложите покупателю/продавцу созвониться с вами по видео-звонку, или позвоните в службу такси попросите доехать водителя до продавца, посмотреть товар;

Также существуют и другие схемы:

1. при использовании онлайн-сервиса поиска автомобильных попутчиков (под предлогом междугородних поездок) Это «Блаблакар»-принцип, как и через сайт «Авито», вам скидывают ссылку, якобы для оплаты поездки, вы переходите, вводите данные карты и лишайтесь денежных средств (суммы разные от 5 000 до 20 000 рублей);
2. представляются руководителями дают указания работникам организации о совершении перевода денежных средств; (совершают

звонок под видом начальника, просят взять всю сумму из кассы и отправить по номерам);

3. под предлогом «выигрыша приза», «возмещения компенсации», «выплаты социальных выплат».
4. Заражение вирусами мобильных телефонов.

Мошенники работают и в социальных сетях:

1. взламывают личные страницы и обманом выманивают денежные средства у граждан;
2. под предлогом возврата утерянной вещи;
3. под предлогом покупки/продажи поддержанных вещей.

В настоящее время мошенники под видом сотрудников банка используют схемы: (понижение процентной ставки по кредиту, уменьшение платежа по ипотеки, рефинансирование кредита, страхование карты).