**«Осторожно - мошенники!**

**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) и звонок от имени оператора сотовой связи.**

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 блокировки банковской карты 4. Под предлогом установки приложения и другие.

Мошенник представляется сотрудником службы безопасности банка (обращается к вам по имени, может назвать ваше 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). 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.

Вторым по популярности приёмом являются звонки абонентам под видом сотовых операторов с предложением продлить якобы истекающий договор на номер телефона. Во время разговора злоумышленник старается отвлечь внимание собеседника обилием технических деталей, после чего уточняет, на какой период клиент желает продлить контракт с оператором. Затем на номер абонента приходит сообщение с кодом, которое необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок». В действительности договоры, заключаемые абонентом с сотовыми операторами, не предусматривают ограниченного срока пользования номером.

Тем временем телефонный мошенник продолжает отвлекать собеседника различными мелкими деталями, пока не спрашивает цифры и код, полученные в сообщении. Затем злоумышленник сообщает, что направил клиенту ссылку, где необходимо ввести код «для завершения дистанционного подписания пользовательского соглашения». Этот код – не что иное, как данные для входа в личный кабинет жертвы на портале Госуслуг. Также мошенники могут попросить внести символическую сумму на счет телефона с помощью банковской карты, после чего происходит хищение всех средств со счета.

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! 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!

***М.А. Кочетков, старший оперуполномоченный ГУР***

***МО МВД России по ЗАТО п. Сибирский,***

***майор полиции***