ОСНОВНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ:

МНИМЫЙ ПОКУПАТЕЛЬ

Получивший широкое распространение способ связан с сайтами объявлений. Мошенники звонят продавцам (чего угодно, начиная от чайников и телевизоров, заканчивая домами и самолетами) и сообщают, что они хотят купить предлагаемую вещь, причем так боятся, чтобы она не досталась другому, что готовы внести предоплату, иногда даже в размере 100% стоимости товара, а подъехать/оформить сделку позже.

Продавец, воодушевленный возможностью наконец-то избавиться от ненужной вещи, конечно, соглашается.

Далее следует просьба дать номер карты. Нормальная, в общем-то, просьба, номер карты отражается везде, начиная от простых магазинов, заканчивая интернет-расчетами во всех видах. Без дополнительных сведений, по одному номеру карты, деньги снять с нее невозможно.

И начинается самое главное в работе мошенников. Финансово грамотные люди, конечно, на такую уловку не поддадутся, но, как известно, «предупрежден – значит вооружен». Мошенник сообщает, что для перевода денежных средств ему необходимо знать дополнительные реквизиты. Иногда это CVV-код, зная который, вместе с номером карты, злоумышленник может сделать покупки в интернет-магазинах, не требующих кода подтверждения.

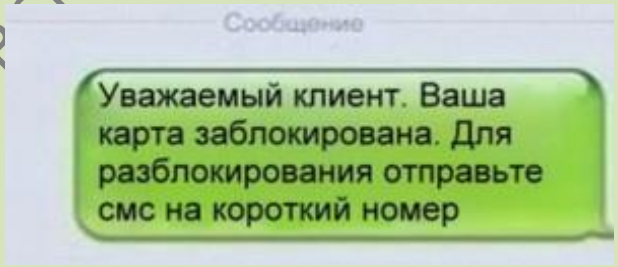
Что делать? Запомнить раз и навсегда: CVV-код (три цифры на обратной стороне карты) и любые пароли из смс должны быть известны только держателю карты. Никогда и ни при каких обстоятельствах они никому не сообщаются. Для предоплаты за товар покупателю достаточно знать номер карты, а уж предложение внести предоплату за дом или автомобиль, не видя предмета торга, должно насторожить продавца сразу же.

НЕ ТОТ, ЗА КОГО СЕБЯ ВЫДАЕТ

Фишинг – выманивание данных карты покупателя путем внедрения вируса в его компьютер или смартфон и замена форм оплаты в интернет-магазинах либо при переводе средств мошенническими, очень сходными с реальными. Таким образом, злоумышленники получают все те же данные о карте – номер, срок действия, CVV-код, которые используют в своих целях.

Что делать? Внимательно изучать формы оплаты, в которые вводятся данные карты. Соединение должно быть защищенным – значок замка и буквы https в адресной строке, в формах оплаты не должно быть каких-либо подозрительных элементов, которых не было ранее. При малейших подозрениях перевод средств или оплату покупки стоит отменить до того, как была нажата кнопка «Оплатить».

ВАША КАРТА ЗАБЛОКИРОВАНА



Мошенник звонит предполагаемой жертве, представляясь сотрудником банка, и сообщает, что ее карта заблокирована, а для разблокировки необходимо назвать Ф.И.О. владельца, адрес, номер телефона, номер карты, CVV-код (иногда выборочно, иногда все эти данные). Далее, конечно же, необходимо назвать ему код из смс.

Дальнейшая судьба средств на карте не отличается от того, что было описано выше. Деньги либо уводятся со счета, либо ими оплачиваются покупки в интернет-магазинах. Вместо звонка «представителя банка» может прийти смс с номера, схожего с номером используемого владельцем карты банка.

Что делать? Все то же – никому и никогда не сообщать личные данные банковской карты.

Все «тайные знания» в виде CVV-кода, паролей, паспортных данных и прочего должны остаться при владельце карты.

ВАШ РЕБЕНОК «ПОПАЛ» В ДТП

Способ давно известный, но тем не менее все еще существующий. Чаще всего на эту «удочку» попадаются пожилые люди. Мошенники звонят предполагаемым жертвам, обычно ночью, и, представившись сотрудником правоохранительных органов, сообщают, что их сын или дочь стали виновниками ДТП либо еще какого-то преступления.

Если пол сына/дочери не совпадает или дитя в это время спокойно спит в соседней комнате, разговор на этом заканчивается. Если же случаются совпадения и жертва продолжает общение, злоумышленник утверждает, что для того, чтобы «замять дело», необходимо перевести на счет мобильного телефона либо номер карты некоторую сумму денег.

Некоторые даже присылают специального человека, который и должен забрать деньги.

Также мошенники могут разговаривать и от имени самого сына или дочери, утверждая, что голос изменился от волнения, травмы и т. д.

Суть одна – в конце разговора всегда будет озвучена просьба о переводе средств.

Что делать? Никогда и никому не переводить деньги. Если все же возникают сомнения – не поддаваться панике, связаться с указанным сыном/дочерью/мужем/ братом.

Как правило, родственник спит и видит сны, не ведая о том, что его используют в качестве наживки.

Обращаться в полицию имеет смысл только если денежные средства уже были переведены, но, увы, шансы их вернуть чрезвычайно малы. Сим-карты, с которых был совершен звонок, окажутся заблокированными и оформленными на подставных лиц, также как и банковские карты, на которые жертву просят перевести деньги.

В 1 полугодии 2021 года на территории Большеуковского района совершено 6 преступлений связаных с хищением денежных средств с банковских карт граждан, и только по 2 преступлениям установлены лица их совершившие.

Прокуратура Большеуковского района Омской области

Как не стать жертвой мошенников?

с. Большие Уки
2021