«Стоит ли доверять?» или «Лейбл решает все!»

С приходом Интернета в нашу жизнь многое изменилось. Например, мы очень часто приобретаем необходимый нам для жизни товар (вещи, бытовая техника, электроника и многое другое) в различных интернет-магазинах считая, что это нам здорово экономит время. Да и лёжа на диване можно приобрести все, что угодно! Здорово ведь совершать покупки не выходя из дома! С другой стороны, мы считаем, что покупки в Интернете экономят не только время, но и деньги! А если еще прикупить себе брендовую вещь, да еще и подешевле!!! Лейбл решает все! Так как промониторив различные сайты можно найти необходимый товар по привлекательной цене! Звучит это все заманчиво, если бы не одно НО!!!

Зачастую мошенники ищут себе жертву в группах по продаже «поддержанных» вещей, либо новых, но по «привлекательной» цене в различных группах и сообществах в социальных сетях. Сегодня речь пойдёт о мошенничествах в социальной сети «ВКонтакте». Так за прошлый год на территории Лунинецкого района зарегистрировано 15 преступлений по ст.209 УК Республики Беларусь (мошенничество) в сети Интернет. К слову все вышеуказанные мошенничества развивались практически по одному и тому же сценарию: потерпевший искал себе какую-либо определенную вещь в различных группах и сообществах по продаже вещей и, рано или поздно, попадался в руки «любезного» мошенника. Далее велась переписка, мошенник всегда вел себя культурно и вежливо, чтобы не вызвать каких-либо подозрений, таким образом втирался в доверие потерпевшему, который вскоре переводил определенную сумму денежных средств на банковскую карту страны, например Зимбабве. Не обращая внимания, что комиссия составляет не малую сумму, да и карта непонятно какого банка. Далее, сам не подозревая этого, просто добровольно переводит деньги, которые долго откладывал на кроссовки с заветным лейблом, человеку у которого нет совести… Но мы не об этом. И, соответственно, далее ты остаешься и без денег и без «товара»…

Есть еще один не менее интересный сценарий. Речь пойдет все о тех же брендовых вещах. Так вот в социальной сети «Вконтакте» существует не мало групп о продаже каких-либо эксклюзивных вещей, а так как это вещь эксклюзивная, то и продать ее нужно соответственно. А значит создаются аукционы, т.е. кто больше предложит, тому и вещь. Гениально! Так вот и в таких случаях мошенники не дремлют, придумывая все новые и новые способы вытянуть как можно больше денежек от доверчивых потенциальных покупателей. И дальше следует следующий сценарий: мошенник выкладывает объявление в такой группе о продаже какой-либо эксклюзивной брендовой вещице (на просторах Интернета легко найти якобы «реальное фото») и тут начинается аукцион. Все бы ни чего, но меня поражает то, что потерпевший сам потом пишет в личные сообщения мошеннику (сам того не подозревая) и

предлагает сумму, которая может заинтересовать. Ох, уж эта человеческая сущность. Уверена, что ни один такой «умный» напишет мошеннику. Ведь те, кто гонится за модой готовы на многое, поверьте. Далее все по старой схеме: дружелюбная, открытая на первый взгляд переписка, в которой мошенник утверждает что он вовсе не мошенник и что завтра-послезавтра он обязательно вышлет посылку на адрес, так сегодня он занят, у него ковид, он экзамене, соревнования, на работе, улетел на Марс и еще много-много различных причин. А ведь после того, как деньги переводятся на банковскую карту общение попросту прекращается.

Исходя из практики меня всегда поражало то, как люди доверяют незнакомому человеку, да еще и не видя его. Ведь за фейковой страницей может скрываться кто угодно. Некоторые потерпевшие даже не спрашивают мобильный номер, чтобы позвонить и обсудить «сделку». Ведь если продавец не мошенник, то ему не сложно ответить на интересующие вопросы по поводу продажи того или иного товара. Логично? У «продавца» часто иностранный номер, поэтому на разговор по телефону он никогда не согласится. А если и соглашается, то телефонный разговор может состоятся через мессенджер (обычно это Viber). Многие привыкли хранить номера в телефонной книге своего мобильного телефона в устаревшем формате — 8029 (025, 033, 044), поэтому, увидев международный вариант +375 29 (25, 33, 44), начинают путаться в цифрах. Этим пользуются мошенники, подбирая похожие: +374 или +372. В длинной череде цифр не обратишь внимания что за номер. Даже +380 почти наверняка пройдет мимо сознания. Это актуально для «развода» на торговых площадках.

Есть еще и другой вариант заполучить Ваши деньги. То есть Вам предлагают перейти по ссылке на сторонние сайты, которые имитируют адреса площадки, где вы размещали объявление, но отличаются доменом первого уровня. То есть это будет не vkontakte.by, а vkontakte.mx — вместо by

окажется что-то другое. Похож, да не он. Адрес может быть еще длиннее — все для отвлечения внимания. Не переходите ни по каким ссылкам, полученным от неизвестных. На «левом» сайте от вас потребуют ввести данные банковской карты: ее номер, срок действия, имя, фамилию и, наконец, CVV. Вся эта информация попадет к мошенникам. Если вы введете ее, вас могут попросить прислать код верификации из SMS — «чтобы уж точно деньги дошли». Примерно в этот момент вы лишаетесь всех денег на карте, которая полностью скомпрометирована.

Вновь пример: посмотрите на любой сервис перевода денег с карты на карту — обычно достаточно номера карты получателя. А вот отправитель указывает все данные — от номера до CVV.

Если все это кажется банальным, будьте уверены: не все такие «продуманные». Расскажите об этих схемах родителям и друзьям. Вы будете удивлены, узнав, как много вокруг доверчивых людей.