В последнее время значительно увеличилось число обращений граждан Немецкого национального района Алтайского края, пострадавших от действий злоумышленников, совершающих хищение денежных средств, совершаемых с использованием глобальной сети Интернет, а также мобильных средств связи, кроме того, по сравнению с 2014 г. значительно возросли и суммы денег, похищаемых у граждан. Так в отношении гр. «Я» с. Гальбштадт осуществлена попытка хищения 127467, 53 рублей, у гр. «З» с. Гришковка похищено 12626, 23 рублей, у гр. «У» с. Гальбштадт 71760 рублей. Это далеко не полный список пострадавших граждан Немецкого национального района от действий злоумышленников.

На сегодняшний день схем, по которым злоумышленники действуют для завладения денежных средств очень много. Последнее так сказать изобретение - это создание вирусов для смартфонов, которые внедряются в системный код различных приложений устанавливаемых на смартфоны, различных файлов, которые скачиваются на телефон при переходе в Интернет браузере телефона по различным сомнительным ссылкам и всплывающим окнам. После чего, если ваша банковская карта подключена к мобильному банку т.е. к сим карте, которая используется в вашем телефоне злоумышленники получают доступ к управлению вашим телефоном и делают это скрытно, то есть осуществляя различные операции по переводу ваших денежных средств находящихся на вашей банковской карте – вы никаких уведомлений из банка не получаете. После чего хищение денежных средств потерпевший обнаруживает случайно, когда зная, что у него на карте имеется некоторая сумма денежных средств идет совершать покупки в магазин, а на кассе при расчете оказывается, что денег нет вовсе, либо обнаруживает отсутствие денег при попытке снять денежные средства с карты.

Чтобы избежать таких ситуаций необходимо быть внимательными при посещении тех или иных интернет сайтов, не переходить по сомнительным ссылкам, не скачивать приложения из сомнительных источников, а устанавливать их только из официальных, предусмотренных производителем источников, такие как «Play Market» - для тех, у кого смартфон под управлением операционная системы «Android», «Marketplace» - для операционной системы «Windows Mobile». Кроме того, нельзя устанавливать интернет браузеры, кроме тех, которые предусмотрены для определенной модели и марки телефона. Также следует отметить, что для защиты своего смартфона необходима установка антивирусных программ, в официальных источниках их имеется различное множество. Также категорически запрещается «привязывать» банковскую карту к каким либо интернет сервисам, «одноклассникам», «вконтакте» и т.п., так как при взломе вашей страницы, злоумышленник через нее сможет получить доступ к банковской карте.

Что делать и как проверить имеются ли в смартфоне вирус и как избежать хищений денежных средств с банковской карты. Самый лучший способ – это вообще не подключать мобильный банк к своей банковской карте, осуществить проверку смартфона на наличие вирусных программ, произвести общий сброс

смартфона, который приводит смартфон в состояние, в котором он был приобретен в магазине.

Также необходимо отметить, что все потерпевшие от хищения денежных средств с банковских карт являются пользователями сотовых связей – «МТС» и «Билайн», реже «Мегафон».

Распространенной сегодня является ситуация, когда граждане, увидев на различных сайтах размещения объявлений «Авито», «Дром» и т.п. созваниваются с лицом, разместившим объявление, договариваются о покупке чего – либо и вносят задаток. После перечисления задатка, продавец перестает отвечать на звонки, становится недоступным и т.п. В таких случаях, если вы все - таки решили рискнуть и перевести кому то деньги в счет задатка, покупки и т.д. то необходимо принять меры к тому, чтобы установить о продавце всю возможную информацию – серию, номер паспорта, кем и когда выдан, место жительства, прописки, посредством интернета получить от него свето копию паспорта, какого либо второго документа удостоверяющего личность, если продавцом выступает организация, то удостоверится в ее действительном существовании – истребовать свето копию свидетельства о регистрации в ИФНС России, также копию паспорта и второго документа удостоверяющего личность. Кроме того, о переводе денежных средств необходимо сохранять подтверждающие документы, в случае хищения денежных средств они будут являться доказательством по делу. Также необходимо связываться с продавцом по «скайпу», чтобы воочию обсудить детали сделки, при этом сделать несколько фото продавца. Эти действия у добропорядочных граждан не вызовут вопросов и они предоставят всю информацию о себе. Если же, напротив, продавец не хочет этого делать, уклоняется от этого, пытается свести все в шутку, то тогда не стоит связываться с таким продавцом вовсе.

Также имеются случаи, когда вы выступаете продавцом и заинтересованный покупатель предлагает перевести задаток на вашу карту и при этом просит сообщить номер карты, срок ее действия и код безопасности, указанный на обороте карты, если таковое имеет место, то нужно сразу понимать, что вы имеете дело с мошенником, так как для перевода денег на банковскую карту необходимо знать всего лишь номер банковской карты и ничего больше! Не соглашайтесь на какие – либо уговоры, о пошаговой процедуре перевода денежных средств - всегда можно узнать по телефону горячей линии, указанной на обороте банковской карты.

Особого внимания заслуживают ситуации, когда мобильный номер был некоторое время подключен к мобильному банку, после чего указанным номером по каким – либо причинам собственник перестает пользоваться, при этом старый номер не отключает от мобильного банка. По истечению некоторого времени, данный номер приобретает новый владелец и обнаруживает, что к нему подключен мобильный банк чужой банковской карты. В связи с этим, необходимо при подключении нового номера к банковской отключать старый номер.

Жители и гости Немецкого национального района, не будьте беспечными при обращении со своими денежными средствами!