О телефонных мошенниках

ОМВД России по Подпорожскому району ЛО доводит до сведения граждан, что участились случаи мобильных мошенничеств.

Используются следующие способы хищения: **обман по телефону** – это требование выкупа или взятки за освобождение знакомого или родственника, якобы, из отделения полиции; **СМС-просьба о помощи** – это просьба перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п... Такие звонки и сообщения рассылаются «в слепую», в большом объёме, в надежде на доверчивого получателя. Цель мошенников – заставить Вас передать свои денежные средства «добровольно».

Есть несколько простых правил, следуя которым Вы сохраните свои денежные средства:

- отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;

- не реагировать на СМС-сообщения без подписи и с незнакомых абонентских номеров;

- внимательно относиться к звонкам с незнакомых номеров.

Если Вы сомневаетесь, что звонивший действительно Ваш друг или родственник, **обязательно перезвоните** на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

В связи с продолжающимися хищениями денежных средств со счетов пользователей банковских карт (в том числе посредствам услуги «мобильный банк»), ОМВД России по Подпорожскому району ЛО доводит до сведения граждан способы хищений, используемые злоумышленниками:

1. Клиент при оформлении банковской карты подключает услугу «мобильный банк». Однако, через некоторый период времени отказывается от номера сотового оператора, не оповещая о данном факте банк. Сотовый оператор автоматически по истечении 3 (иногда 6) месяцев данный номер передает следующему клиенту. Таким образом, СМС-сообщения о состоянии счета от банка идут третьему лицу, который используя стандартные комбинацию, может использовать денежные средства, находящиеся на банковской карте, не принадлежащей ему.

2. Используемое мобильное устройство «инфицировано вирусом» (варианты инфицирования различны: всплывающие окна, СМС-рассылка, использование нелицензионных программ, непроверенных носителей, переходы по интернет-ссылкам и прочие). Данные клиента становятся доступны злоумышленникам, которые в свою очередь получают доступ к мобильному устройству и возможность воспользоваться денежными средствами со счета банковской карты. Для предотвращения данной ситуации необходимо на своих мобильных устройствах, имеющих возможность выхода в Интернет, установить Антивирусные программы.

3. Некомпетентность клиента, использующего услуги «Сбербанк ОнЛайн». А именно, при входе в систему «Сбербанк ОнЛайн», через пораженное вирусом устройство, а также используя «всплывающие окна», самостоятельно вводит конфиденциальную информацию (№ банковской карты, пин-код, номер телефона). На официальном сайте **НИКОГДА** не запрашивается данная информация, ПАО «Сбербанк России» первоначально формирует клиентскую базу и в дальнейшем не запрашивает данные сведения. Для предотвращения данной ситуации необходимо на своих компьютерах, планшетах, смартфонов и т.д. установить Антивирусные программы.

4. Введение в заблуждение клиента банковской карты Сбербанка. А именно, в сети интернет имеется множество сайтов, на которых можно приобрести товары и оплатить их с помощью банковской карты. Злоумышленники, заказывая товар через интернет, указывают номер сотового телефона, якобы принадлежащий им (выдуманный), на который впоследствии высылается СМС-уведомление с пин-кодом, необходим для подтверждения операции по банковской карте. Вам на телефон приходит данное СМС-уведомление и через некоторый период времени Вам звонит третье лицо, которое вводит Вас в заблуждение с целью получения данного пин-кода. В случае, если Вы сообщаете данному лицу код, то оно имеет возможность произвести данную оплату товара, используя Вашу банковскую карту.

5. Отправка денежных средств клиентом самостоятельно. На Ваш телефон приходит СМС-сообщение о том, что Ваша банковская карта заблокирована, с просьбой перезвонить «сотруднику банка по номеру телефона», либо злоумышленник звонит на Ваш телефон сам и представляется сотрудником банка. Далее вы выполняете требования якобы «сотрудника банка» для разблокирования карты, а на самом деле отправляете денежные средства на счет злоумышленников.

6. Передача персональных данных третьим лицам. В социальных сетях («В контакте», «Одноклассники» и т.п.) приходит сообщение от, якобы, вашего знакомого или родственника о том, что ему необходимо провести какую-либо операцию со своими денежными средствами, но для этого ему необходим номер Вашей банковской карты. А после передачи Вами номера банковской карты, «знакомый (родственник)» просит, якобы для подтверждения операции, переслать поступивший на Ваш телефон специальный код. На самом деле в социальной сети Вам пишет не Ваш знакомый или родственник, а мошенник, получивший доступ к его страннице. Также мошенники получают от Вас номер карты через интернет-магазины. Как только Вы передаете третьему лицу номер вашей банковской карты, это лицо уже может совершать платежи со счета вашей карты, зная Вашу фамилию и имя. А сообщив злоумышленнику, поступивший на Ваш телефон код, Вы даете ему доступ в Ваш «Личный кабинет Сбербанк ОнЛайн», где он может совершать любые операции от Вашего имени.

НЕ РЕКОМЕНДУЕТСЯ:

- перезванивать на незнакомые номера;
- переходить по неизвестным интернет-ссылкам;

- отвечать на СМС-сообщения, вызывающие сомнения;

- передавать Ваши конфиденциальные данные третьим лицам;

- сообщать сведения, содержащиеся в СМС-сообщениях, которые пришли на Ваше мобильное устройство третьим лицам.

ПОМНИТЕ: сотрудники банка **НЕ** отправляют СМС-сообщения и **НЕ** обзванивают клиентов с личных мобильных телефонов. Официальные номера ПАО «Сбербанк России»: **8-800-555-55-50, +7-495-500-55-50 и 900. Только с указанных номеров с Вами могут связаться сотрудники Банка.**

НАСТОЯТЕЛЬНО РЕКОМЕНДУЕМ:

- отказаться от услуги «мобильный банк», если мобильный телефон используется Вами для выхода в сеть Интернет.

- перезванивать своим родственникам и знакомым по имеющимся у Вас номерам и уточнять необходимость перевода денежных средств

- исключить передачу третьим лицам Ваших персональных данных (номер счета, номер карты и т.п.).

При утрате сим-карты, на абонентский номер которой подключена услуга «мобильный банк», необходимо незамедлительно сообщить об этом в банк.

Схемы мошенничества видоизменяются и становятся все более изощренными с каждым днем. Однако есть основные, самые распространенные схемы, по которым действуют современные аферисты на Авито:

- покупка по предоплате с последующей отправкой товара службой доставки;

- снятие денег с кредитной карты по предоставленным секретным кодам, которые сам продавец передает в руки мошенников;

- покупка автомобиля через интернет чревата различными опасностями, о которых покупатель может узнать не сразу;

МОШЕННИЧЕСТВО С ПРЕДОПЛЛТОЙ.

Пожалуй, самый старый, но и самый распространенный способ мошенничества - это предоплата за несуществующий товар. Схема такова: мошенник дает объявление о продаже чего-либо, при этом оговаривается, что передать товар при личной встрече он никак не может в виду большой занятости. Но после вашей предоплаты на банковскую карту продавец, так и быть, согласен отправить вам товар по почте. Как можно обезопасить себя от нечестных продавцов в данном случае: смотрите наличие реальных фотографий в объявлении, при появлении каких-либо сомнений, просите продавца сделать дополнительные фото в разных ракурсах. Если у продавца внезапно сломался фотоаппарат - просите о видеозвонке в Skype. Это даст вам возможность убедиться в том, что товар в действительности существует. «Пробейте» телефон продавца через различные поисковые системы: Google, Yandex, Yahoo. Конечно, мошенники могут на каждую аферу менять сим-карту, но иногда номера телефонов успевают «засветиться» в интернете, где уже попавшиеся на удочку мошенников покупатели оставляют свои отзывы. При осуществлении дорогостоящей покупки дистанционно настаивайте на наложенном платеже - в

таком случае вы вносите оплату в офисе службы доставки, после того, как получаете товар. Это будет стоить вам дополнительных расходов, однако это небольшая плата за ваше спокойствие и уверенность в том, что вас не обманут, но даже «наложенным платежом» Вы можете приобрести «кота в мешке».

НОВЫЙ СПОСОБ С КРЕДИТНОЙ КАРТОЙ.

Относительно новый способ мошенничества, который рассчитан на тех, кто продает товары через интернет. Вы выставляете товар через Авито, спустя определенное время объявляется покупатель, который согласен его приобрести, и все его устраивает, и деньги он согласен перевести немедленно. После получения реквизитов на оплату мошенники тем или иным путем попытаются выведать у вас секретные данные, которые откроют им доступ к денежным средствам на вашей карте. Помните, ни при каких обстоятельствах нельзя передавать третьим лицам секретную информацию, размещенную на обратной стороне вашей банковской карты, а также передавать коды, которые приходят вам на телефон в СМС. Также не следует подходить к банкомату и вводить данные, которые вам передают мошенники. Поступая так, вы предоставляете мошенникам доступ к своим деньгам. Если карта дебетовая вы потеряете кровно заработанные, если кредитная – приготовьтесь оплачивать кредиты, которые вы не брали. Как себя обезопасить? Для осуществления платежа через банк, в котором открыта карта получателя, достаточно следующей информации: ФИО держателя и номер карты. Для платежа через другой банк могут понадобиться другие реквизиты, их можно узнать у службы поддержки банка.

ПРОДАЖА АВТО.

Покупка автомобиля через интернет может принести много неприятных неожиданностей, если как следует не подготовиться и не прояснить некоторые моменты. С автомобилями, приобретаемыми с рук, следует быть особенно осторожным, проверять необходимо все - от состояния двигателя до документов на нее. Помимо тест-драйва неплохо бы заехать на ближайшую СТО и доверить дело профессионалам - они смогут выявить проблемы, которые просто невозможно уловить при поверхностном осмотре. Также стоит тщательно осмотреть документы и проверить их на подлинность - иначе при первой же проверке ДПС вы можете выяснить, что машина числится в угоне, или является залоговым имуществом и подлежит изъятию в пользу неизвестного кредитора.