**Будьте бдительны!**

С начала года на территории обслуживания Межмуниципального отдела МВД России «Ханты-Мансийский» зарегистрировано более 300 фактов мошенничества, совершенных посредством сети Интернет. Анализ складывающейся на территории города Ханты-Мансийска и Ханты-Мансийского района оперативной обстановки свидетельствует об увеличении числа мошенничеств, совершенных с использованием новых технологий и высокотехнологичных устройств — компьютеров, пластиковых карт, мобильных телефонов.

**Телефонное мошенничество.**

Цель мошенников — заставить граждан передать свои денежные средства «добровольно». Они хорошо знают психологию людей и используют следующие мотивы: беспокойство за близких и знакомых, беспокойство за свой телефонный номер, счёт в банке или кредитную карту, любопытство — желание получить доступ к SMS и звонкам других людей.

***Ситуация 1:*** *Вам от имени оператора приходит SMS-сообщение с текстом, сообщающим о поступлении на Ваш счет определенного количества средств. Пока Вы задаетесь вопросами, как и откуда, могли прийти деньги, приходит другое SMS-сообщение с текстом, что деньги внесли на Ваш счет по ошибке и просят вернуть такую же сумму на «правильный» абонентский номер. Либо человек, «ошибочно положивший Вам деньги на телефон», звонит лично и вежливо, но весьма настойчиво просит вернуть средства. Многие попадаются на этот обман, потому как суммы здесь фигурируют небольшие.*

**Как поступать в такой ситуации.** Проверьте баланс Вашего счета, чтобы удостовериться, что он был пополнен на запрашиваемую незнакомым человеком сумму.

***Ситуация 2:*** *вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной — помощь другу, изменение тарифов связи, проблемы со связью и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь — и оказывается, что с Вашего счёта списаны крупные суммы.*

*Другие варианты этого вида мошенничества выглядят так. Абоненту приходит SMS-сообщение, содержащее объявление с предложением стабильной работы с высокой зарплатой. Для получения информации о работе предлагается отправить SMS или позвонить на короткий номер (повышенная стоимость SMS или платный автоответчик!).*

*Приходит SMS, что Вы подписаны на какую-то услугу (получение прогноза погоды и т.п.) несколько дней бесплатно. Чтобы отключиться, нужно набрать сообщение STOP на такой-то четырехзначный номер. Если отправите SMS, то денег на счету заметно поубавится.*

**Как поступать в такой ситуации.** Единственный способ обезопасить себя в этой ситуации — не звонить по незнакомым номерам и не отправлять SMS.

***Ситуация 3:*** *мошенники рассылают владельцам мобильных устройств сообщения с предложением загрузить «открытку», «подарок» и т.п. перейдя по Интернет-ссылке. Переходите по ссылке — и со счёта списывается часть денег, или в телефон загружается вирус, который проникает в программное обеспечение телефона и, используя сотовую связь, а именно абонентский номер, который привязан к банковской карте (услуга «Мобильный банк») происходит списание денежных средств со счета банковской карты. Злоумышленник получает полный доступ к «Мобильному Банку» потерпевшего, при этом СМС-сообщения о списании денежных средств не всегда поступают на телефон потерпевшего.*

**Как поступать в такой ситуации.** Не открывайте вложенные файлы и не переходите по ссылкам.

***Ситуация 4:*** *Вам поступает звонок, либо приходит SMS-сообщение, якобы, от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными: предложение подключить новую эксклюзивную услугу; для перерегистрации во избежание отключения связи из-за технического сбоя; для улучшения качества связи; для защиты от СПАМ-рассылки; предложение принять участие в акции от Вашего сотового оператора. Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п. На самом деле код, который Вам предложат отправить, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.*

**Как поступать в такой ситуации.** Критически относитесь к таким сообщениям и не спешите выполнить то, о чем просят. Лучше позвоните в сервисную службу своего оператора связи, сообщите о пришедшей на Ваш телефон информации и узнайте, какая сумма спишется с Вашего счета при отправке SMS или звонке на указанный номер.

***Ситуация 5:*** *абонент получает на мобильный телефон SMS-сообщение с неизвестного телефона примерно следующего содержания: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.*

**Как поступать в такой ситуации.** Не реагировать на СМС с незнакомых номеров о материальной помощи. Постарайтесь связаться со знакомым по известному Вам номеру и уточнить, есть ли у него проблемы с отключением телефона.

**Мошенничества с банковскими картами.**

Простота использования банковских карт оставляет множество лазеек для мошенников. Например, Вам приходит сообщение с текстом: «обслуживание вышей банковской карты заблокировано, за подробной информацией обращайтесь по телефону...». После того, как граждане перезванивают на указанные номера, мошенники представляются сотрудниками банков, «в котором у Вас открыт счет», и, используя определенную терминологию, сообщают, что в целях исключения блокировки банковской карты и других нежелательных действий необходимо немедленно протестировать карту через банковский терминал и произвести ее активацию. При выполнении дальнейших указаний злоумышленников с банковских карт граждан списываются значительные денежные суммы.

Происходит следующее: Вы, выполняя указания мошенников, сами не замечая, сообщаете злоумышленникам реквизиты своей банковской карты (цифры на лицевой и оборотной стороне, срок действия и даже ПИН-код), в результате они получают доступ к Вашему счету.

Разновидностью указанного способа мошенничества является также рассылка SMS-сообщений с информацией о снятии денежных средств и указанием номера телефона для справок.

**Как поступать в такой ситуации:**

* Не торопитесь сообщать реквизиты вашей карты, ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои персональные данные.
* Помните, без Вашего согласия карту никто и никогда не может заблокировать, а чтобы устранить любую банковскую неполадку, Вам лично нужно присутствовать в банке, а не перечислять деньги на чужие счета и номера сотовых телефонов.
* Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться Банком.

**Полицейские просят граждан быть более бдительными и осторожными при продаже и покупке товара посредством сети Интернет.**

**Информация о мерах безопасности публикуется на таких популярных сайтах, как «Авито» и «Дром.ру».**

**Прислушайтесь к советам профессионалов! И помните: для перевода денежных средств с карты на карту достаточно назвать номер банковской карты, указанный на лицевой стороне. Храните втайне от посторонних лиц ПИН-код вашей карты, ее номер на обратной стороне и ни в коем случае не сообщайте четырехзначный код, присылаемый мошенниками в тексте** **СМС.**