Уважаемые граждане!

Несмотря на принимаемые сотрудниками полиции меры по организации профилактической работы, направленной на предупреждение мошенничеств в сфере информационно-телекоммуникационных технологий и краж денежных средств с банковских карт[1], количество преступлений данного вида продолжает увеличиваться.

Руководство Межмуниципального отдела МВД России «Полярнозоринский» выражает крайнюю озабоченность ситуацией складывающейся в сфере противодействия мошенничествам, которая, несмотря на принимаемые меры всё ещё остаётся сложной. В настоящее время на территории РФ широко распространены многочисленные виды мошенничеств, совершаемые с использованием средств телефонной связи и сети Интернет, из которых можно выделить:

1. Мошенничества, совершаемые посредством сети Интернет через социальные сети («ВКонтакте», «Одноклассники» и другие), когда злоумышленники «взламывают» персональную страницу гражданина в социальной сети и от его имени рассылают сообщения родственникам и знакомым с просьбами о переводе денежных средств на различные нужды.
2. Мошенничества, совершаемые посредством сети Интернет через сайты объявлений (например «Авито», «ВКонтакте» и другие), когда злоумышленник, выступая в роли покупателя какого-либо товара размещённого гражданином, звонит ему на указанный в объявлении телефон и просит перевести денежные средства под различными предлогами.
3. Мошенничества, совершаемые посредством сети Интернет через различные ненадёжные сайты, а также в социальных сетях, когда гражданин, желая приобрести товары по низкой цене, заранее переводит денежные средства злоумышленнику.
4. Мошенничества,совершаемые посредством телефонных соединений, когда злоумышленники звонят гражданину и сообщают сведения о якобы попавших в «беду» родственниках или знакомых (ДТП, проблемы с полицией и другое), после чего следуют требования о переводах денежных средств.
5. Мошенничества, совершаемые посредством направления гражданину СМС - сообщений содержащих сведения о блокировании принадлежащей ему банковской карты и последующими за этим просьбами подойти к ближайшему банкомату и произвести какие-либо операции с банковской картой.
6. Мошенничества, совершаемых посредством телефонных соединений, когда злоумышленники звонят гражданину и сообщают сведения о том, что ранее приобретённые им лекарственные препараты, так называемые БАДы, якобы были некачественные и, что гражданину полагается денежная компенсация, после чего следуют просьбы о переводах денежных средств.

Всё вышеперечисленное - это **МОШЕННИЧЕСТВО**, переводить денежные средства нельзя ни в коем случае! Никаких разговоров и переписки с мошенниками не вести. Никому не сообщать сведений по персональным счетам и банковским картам. Заказывать товары исключительно на проверенных Интернет сайтах без предоставления предоплаты.

Основные виды мошенничеств, совершаемых с применением технологии дистанционного платежа:

- Объявление о продаже: Мошенники-продавцы просят перевести деньги за товар, который впоследствии жертва не получает.

- Звонок о несчастном случае: Мошенники звонят жертве от лица близкого человека или представителя власти и выманивают деньги.

- Объявление о покупке: Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

- Блокировка банковской карты: Сообщение о блокировке банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

---

[1] Далее – ИТТ.

- Получение выигрыша (компенсация за потерянный вклад): Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату «за сохранность денег».

- Сообщение от друзей: Мошенник пользуется чужой страницей в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные карты жертвы якобы для перечисления денег под различными предлогами.

- Вирус в телефоне: Мошенники внедряют вирус в телефон жертвы, предлагая пройти по «зараженной ссылке» (в том числе от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону.

- Звонок сотрудника правоохранительных органов. Жертва получает звонок якобы от сотрудника полиции (ФСБ, Следственного Комитета, Прокуратуры) о том, что неизвестный пытался снять деньги с ее счета или оформить кредит, либо ее личные данные были «слиты» банковскими сотрудниками, в связи с чем необходимо деньги перевести на «безопасный счет». Основная цель – заполучить деньги потерпевшего.

Способы защиты от мошенничеств, совершаемых с применением технологии дистанционного платежа:

- Не сообщать третьим лицам номера счетов, банковских карт и их реквизиты, логины и пароли от личных кабинетов, коды подтверждения операций, указанных в поступающих смс-сообщениях;
- Перед тем как осуществить операции по переводу денежных средств неизвестному лицу, представившемуся родственником, другом, знакомым, попавшим в трудную ситуацию, связаться с ним иным способом для подтверждения его просьбы;
- Если сообщили, что банковская карта заблокирована или по счету происходят операции по переводу денежных средств, которые собственником не совершались, обратиться в отделение банка, в котором обслуживается банковский счет или по номеру телефона службы поддержки, указанному на оборотной стороне банковской карты, не выполнять указания лица, представившего сотрудником банка;
- Не использовать мобильный телефон с подключенной услугой «Мобильный банк» для выхода в интернет **без установленных антивирусных программ**, не переходить по неизвестным ссылкам, указанным в рекламных сообщениях, так как при этом на телефон может быть загружено вирусное программное обеспечение, в результате чего может произойти списание денежных средств со счета принадлежащей банковской карты;
- Не перечислять денежные средства при совершении покупок в интернет-магазинах или на иных интернет-сайтах, приложениях и социальных сетях («Авито», ВКонтакте, «Одноклассники»), не убедившись в благонадежности контрагента. Внимательно изучить рейтинг контрагента на доске объявлений, отзывы других покупателей, информацию о нем в сети Интернет;
- Не пользоваться услугами непроверенных и неизвестных сайтов по продаже билетов, путевок, бронирования отелей и т.д. Обращать внимание на электронные адреса сайтов известных компаний и агентств, так как имеются сайты-клоны, со схожими адресами, зачастую отличающимися одним символом, используемые для мошеннических действий;
- Не размещать в открытом доступе и не передавать посторонним информацию личного характера. Данная информация может быть сохранена злоумышленниками и впоследствии использована в противоправных целях;
- Не перечислять денежные средства под предлогом активации выигрышей в различных рекламных акциях, лотереях, розыгрышах и т.д.;
- Помнить, что для перечисления денежных средств на счет банковской карты, достаточно знать только ее номер, не сообщать никому другой дополнительной информации и не подключать услугу «Мобильный банк» к иному номеру.
- Немедленно прекратить входящий звонок, если дело касается финансов, и самостоятельно перезвонить в ту организацию, из которой он якобы поступил;
- Не переводить деньги на так называемые «безопасные счета».

Межмуниципальный отдел МВД России «Полярнозоринский»