«КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ»

Активное развитие современных информационно-коммуникационных технологий, наряду с выполнением общественно-полезных функций, порождает новые угрозы как государственной, так и общественной безопасности.

Одновременно с ростом количества телекоммуникационных устройств и пользователей информационных сетей увеличивается число потенциальных жертв, а также возрастают возможности эксплуатации сети «Интернет» и различных высокотехнологичных устройств для совершения преступлений.

Озабоченность в данной ситуации вызывает высокая латентность данных преступлений, которая обусловлена анонимностью в сети «Интернет» и отсутствием непосредственного контакта с потерпевшим, охватом широкой аудитории, простотой доступа к информации, а также организованным и трансграничным характером посягательств.

В настоящее время практически каждое седьмое преступление совершается в сфере информационно-коммуникационных технологий или с использованием компьютерной информации, в том числе с применением расчетных пластиковых карт, компьютерной техники, сети «Интернет» и средств мобильной связи.

Чаще всего такие преступления связаны с хищением чужого имущества (ст.ст. 158 и 159 Уголовного кодекса Российской Федерации).

На территории Александровского района, как и по всей стране, количество зарегистрированных преступлений, связанных с хищением денежных средств с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации на протяжении последних лет растет. Если в 2019 году на территории района было зарегистрировано 116 подобных преступлений, то за 2020 год – 148. В текущем году по сравнению с прошлым годом количество хищений, совершенных дистанционно, возросло с 52 до 98.

Установление лица, совершившего преступление, вызывает серьезные трудности при расследовании уголовных дел рассматриваемой категории.

Как правило, подобные преступления совершаются с использованием компьютерной техники, мобильных устройств, специальных средств, позволяющих изменять абонентский номер телефона, что позволяет совершать их при отсутствии непосредственного контакта потерпевшего с преступником, то есть в условиях полной анонимности.

На протяжении последнего времени распространена практика хищения денежных со счетов держателей банковских карт при поступлении звонка якобы от представителя кредитной организации.

При совершении преступления преступник звонит жертве и представляется сотрудником кредитной организации, сообщает о том, что с банковского счета потерпевшего осуществлена попытка хищения денежных средств, либо осуществлен несанкционированный доступ к личному кабинету. После этого, в ходе разговора, войдя в доверие, под различными предлогами получает информацию о номере банковской карты, персональных данных, различных кодах доступа и

паролях, что позволяет без лишних усилий распоряжаться денежными средствами потерпевшего, находящимися на его банковском счету. Выяснив у жертвы необходимые сведения, мошенник с помощью различных сайтов и приложений может свободно переводить деньги потерпевшего со счета на счет или с их помощью оплачивать покупки.

Как можно заметить, схема мошенничества является очень простой, однако наши граждане сами предоставляют возможность мошенникам похитить денежные средства, сообщая всю необходимую тем информацию. Мошенники легко входят в доверие жертвы, представляясь сотрудниками банка и обращаясь к потерпевшему по имени и отчеству, что создает видимость того, что разговор действительно ведет представитель банка. Вместе с тем узнать номер банковского счета или данные владельца банковской карты в современных условиях не составляет никакого труда (в целях безопасности способы получения таких данных в данной статье не сообщаются).

В данной ситуации следует придерживаться ряда простых правил, связанных с охраной своих персональных данных, номеров банковских карт и банковских счетов, различных паролей и кодов доступа:

1. Если Вам позвонили по телефону и представились сотрудником банка, сообщив, что в данную секунду совершается хищение Ваших денежных средств или неправомерного доступа к Вашим данным, Вы не обязаны вести разговор по телефону. Успокойтесь. Вас, возможно не обманывают, что с Вашей карты совершается хищение денежных средств, только в данной ситуации не говорят, что хищение совершает сам звонящий. В данной ситуации Вы можете вежливо сообщить, что обратитесь в ближайшее отделение банка с данным вопросом. Разговаривать с мошенником не имеет никакого смысла. Кроме того, по вопросам хищения денежных средств, как правило, сотрудники банка клиентам не звонят.

2. Никогда не сообщайте незнакомым людям номера своих банковских карт, персональные данные, пароли и коды доступа. Те, кто знаком с оплатой покупок в сети «Интернет» знает, что для оплаты такой покупки необходимы реквизиты банковской каты и специальный CVC-код, расположенный на оборотной стороне банковской карты. Данные CVC-кода обеспечивают доступ к Вашему банковскому счету и являются своего рода Вашей электронной подписью. Указанный код нельзя никому сообщать, в том числе сотрудникам банка.

3. При совершении покупок в сети «Интернет» пользуйтесь только официальными и проверенными временем сайтами, потому что оставленные Вами персональные данные, в том числе номера банковских карт и любая другая информация может оказаться в открытом доступе и быть использована мошенниками.

4. Осторожней относитесь к сайтам и информации о полагающихся гражданам компенсационных выплатах и просьбам сообщить номера имеющихся банковских карт «для перевода компенсации». Информацию о причитающихся Вам компенсациях Вы можете уточнить в государственных органах. Помните: бесплатный сыр бывает только в мышеловке.

Александровская городская прокуратура

2021 г.