Профилактика преступлений в сфере информационных технологий

Развитие информационных технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи информационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение запрещенной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Среди наиболее распространенных способов хищений следственная практика выделяет:

- использование злоумышленниками индивидуальных данных банковских карт пострадавших для осуществления расчетов в преступных целях;

- двойное списание, характеризующееся тем, что потерпевший передает банковскую карту другому лицу (продавцу, оператору, официанту и др.), которую тот дважды проводит через платежный терминал под предлогом ошибки при первоначальном платеже;

- хищение при бесконтактной оплате, в тех случаях, когда похитители оперируют собственными бесконтактными считывателями или терминалами, прислоняя их к карманам и сумкам;

- хищение с использованием дубликата сим-карты мобильного телефона, которое осуществляется путем предварительного выяснения преступниками номера сим-карты, к которому привязаны банковские карты и изготовления ее фальшивого аналога с последующим списанием денежных средств;

- хищения посредством использования информации о банковских картах, предоставленных похитителям самими пострадавшими для оплаты продаваемых ими товаров;

- распространенный характер носят хищения, связанные с обманом доверчивых граждан, когда похитители, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившихся в их жизни неблагоприятных ситуаций;

- отмечены случаи мошенничества, при которых похитители просят о перечислении денежных средств или оказании возмездных услуг под предлогом различных нужд органов государственной власти, а также правоохранительных органов.

Данные деяния могут квалифицироваться по п. «г» ч.3 ст. 158 УК РФ, либо по ст. 159.3 УК РФ. Эти составы очень схожи и являются смежными. Однако отграничению таких смежных преступлений как кража имущества с банковского счета и мошенничество с использованием электронных средств платежа будет способствовать анализ объективной стороны совершенного преступления.

Так, отличия здесь заключаются в следующем:

1. При краже действия виновного должны быть тайными, в то время как при совершении мошенничества преступник действует открыто, общаясь с потерпевшим или иным лицом.

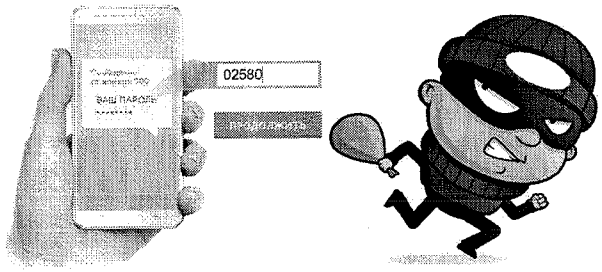
2. При краже потерпевший или иное лицо не участвует в процессе изъятия похищаемого имущества, а при мошенничестве виновный посредством обмана понуждает другое лицо передать похищаемое имущество или совершать действия способствующие изъятию имущества.

Сегодня одним из самых распространенных способов завладеть деньгами граждан является мошенничество с банковскими картами.

Использование банковской карты значительно упрощает операции с деньгами, но одновременно открывает обширные горизонты для злоумышленников.

Чтобы не стать жертвой обмана обеспечьте защиту своих средств, для чего можно использовать следующие рекомендации:

Никому и никогда не сообщайте пароли,
которые приходят на ваш телефон.
Любой запрос пароля под любым предлогом - это мошенничество



Также никому не сообщайте данные вашей банковской карты.
Для перевода средств достаточно передать номер карты.
Никогда не передавайте
срок действия карты и цифры с обратной стороны карты.

1.Не следует ни при каких обстоятельствах сообщать посторонним лицам ПИН-код, а также записывать его на бумаге и хранить рядом с картой.

2.Не стоит совершать покупки на сайтах, не внушающих доверия.

3.Не рекомендуется держать на карте, предназначенной для интернет-покупок, большие суммы.

4.Снятие средств лучше осуществлять непосредственно в офисах финансовой компании (рядом с ними), потому что территория около банка и внутри него просматривается камерами слежения.

5.Не стоит стесняться закрывать от посторонних клавиатуру банкомата при введении ПИН-кода.

6.Не следует прибегать к помощи посторонних в случае возникновения сложностей при снятии денег, правильнее обратиться непосредственно к сотрудникам банка.

7.При открытии счета следует обратить внимание на возможность оформления страховки банковской карты. Такая услуга в ряде случаев позволяет вернуть денежные средства.

8.Не перезванивайте на мобильный номер с сомнительным текстом. Все номера для связи банк указывает в открытом доступе. Также номер телефона технической поддержки указан на оборотной стороне Вашей карты.

9.В случае если SMS-сообщение о блокировке карты действительно получено от банка, в тексте сообщения всегда указаны первые и последние 4 цифры номера Вашей карты. В SMS-сообщениях мошенников номер карты не указан, он им неизвестен!

10.При утере карты срочно обратитесь в банк для немедленной блокировки.

11.Не реже раза в месяц получайте выписку по счету и проверяйте ее.

Если Вы стали жертвой мошенников – незамедлительно обращайтесь с заявлением в полицию.

В связи с вышеизложенным, настоятельно рекомендуется сохранять бдительность, не откликаться на такие провокации и в каждом случае поступления сомнительных предложений от неизвестных лиц сообщать о них в компетентные органы для уголовно-правовой оценки и организации уголовного преследования злоумышленников.

Анадырская межрайонная прокуратура,
2020 год