ПАМЯТКА

«Не стань жертвой мошенничества с банковской картой»

Прокуратура города Черкесска
КЧР, г. Черкесск, Площадь Кирова, 18.

Понятие мошенничества содержится в статье 159 Уголовного кодекса Российской Федерации – это хищение чужого имущества или приобретение права на имущество путем обмана или злоупотребления доверием.

Статьей 159.3 Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за мошенничество с использованием электронных средств платежа.

Электронное средство платежа – это средство или возможность осуществлять безналичные денежные переводы с применением электронных носителей информации или информационных технологий. Наиболее распространенное электронное средство платежа – банковская карта.

Банковская платежная карта – пластиковая карта, привязанная к одному или нескольким расчетным счетам в банке, используется для оплаты товаров и услуг, в том числе через сеть Интернет, а также снятия наличных. За счет простоты использования банковских карт, у мошенников возникает множество способов для обмана.

Мошенничество с использованием банковских карт относится к категории трудно раскрываемых. Потерпевшим может стать любой человек, имеющий банковский счет, привязанный к банковской карте и потерявший бдительность или внимательность.

Данное преступление может совершить любое лицо, имеющее необходимые навыки.

Мошенники втираются в доверие к гражданам, представляются сотрудниками банков или правоохранительных органов, обещают лёгкую прибыль, получают необходимые сведения, после чего совершают хищение денежных средств со счета потерпевшего.

Защититься от подобного рода обмана возможно, проявляя бдительность и адекватно оценивая ситуацию.

Общими признаками, которые должны насторожить и обратить Ваше внимание в ходе пос Общими признаками, которые должны насторожить и обратить Ваше внимание в ходе поступившего звонка или сообщения, являются:

- незнакомый номер, с которого происходит звонок или поступило сообщение;

- особая манера общения, а именно, нагнетание обстановки, обилие в лексиконе слов «срочно», «быстро», «немедленно, «нужно как можно скорее». Целью злоумышленников является застать Вас врасплох, не дать времени на обдумывание. Во время телефонного разговора мошенник, ведет себя всегда уверенно, может давить, настаивать или, наоборот, любым способом пытаться расположить к себе абонента, чтобы выманить информацию;

- отсутствие четких, прямых ответов на ваши вопросы;

- требования сообщить какую-либо секретную персональную информацию или личные данные (номер и ПИН-код банковской карты, персональные сведения, пароли на сайте и пр.);

тупи

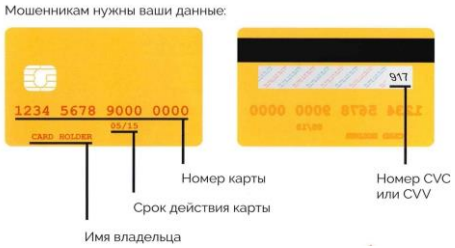
вшего звонка или сообщения, являются:

- незнакомый номер, с которого происходит звонок или поступило сообщение;

- особая манера общения, а именно, нагнетание обстановки, обилие в лексиконе слов «срочно», «быстро», «немедленно, «нужно как можно скорее». Целью злоумышленников является застать Вас врасплох, не дать времени на обдумывание. Во время телефонного разговора мошенник, ведет себя всегда уверенно, может давить, настаивать или, наоборот, любым способом пытаться расположить к себе абонента, чтобы выманить информацию;

- отсутствие четких, прямых ответов на ваши вопросы;

- требования сообщить какую-либо секретную персональную информацию или личные данные (номер и ПИН-код банковской карты, персональные сведения, пароли на сайте и пр.);



Наиболее распространёнными видами мошенничеств с банковской картой являются:

«Объявления…»

Приобретая товары и услуги через сайты бесплатных объявлений:

- не вносите предоплаты за товар;

- оплачивайте товар при личной встрече и после его проверки;

- не сообщайте персональные данные банковской карты;

- проверяйте полученную информацию посредством сети Интернет.

Явными признаками мошенника являются:

- потенциальный покупатель звонит из другого региона;

- человек соглашается купить товар не глядя;

- покупатель не соглашается на другие формы оплаты, кроме электронного платежа;

- покупатель не готов встречаться лично, не говорит адрес доставки товара и прочие данные;

«Подозрительные смс…»

При получении подозрительных смс-сообщений, таких как: «На ваш счет зачислено 30 000 рублей. С уважением, Ваш банк», а через несколько минут перезванивают и говорят, что ошиблись и случайно зачислили на вашу карту деньги, просят вернуть их обратно.

Ваши действия: предложите звонящему, обратиться в свой банк и решить вопрос самостоятельно. Не переводите никому никаких денежных средств.

Кроме этого, смс-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру…».

Ваши действия: обратиться в свой банк для проверки поступившей информации, не перезванивать по указанному в смс-сообщении номеру.

«Звонок из банка…»

Злоумышленники звонят гражданам, представляясь сотрудниками банков, называя их по имени, отчеству, просят сообщить данные банковских карт (номер, CVC(CVV), PIN-коды и т.п.),

установить программы удаленного доступа, перевести денежные средства на «защищенный счет» для предотвращения якобы несанкционированного списания денежных средств, либо оформления кредита.

Запомните: сотрудники банка никогда не спрашивают данные банковских карт. Необходимыми сведениями сотрудник банка располагает. В случае, если же какая-либо проблема действительно возникнет, настоящим сотрудником банка вам будет рекомендовано обратиться в ближайшее отделение банка лично, для решения всех вопросов.

«Социальные работники …»

Злоумышленники представляются соцработниками и сообщают о надбавке к пенсии, перерасчете квартплаты, премии ветеранам, срочном обмене денег на дому, якобы «только для пенсионеров».

Не верьте, это мошенники! Без официального объявления не может проводиться никакой «срочный обмен денег».

«ВКонтакте» (взлом страниц)

Со страницы друзей, знакомых, родственников злоумышленники отправляют сообщения с просьбой одолжить денег на неотложные нужды, сообщают о потере близкого родственника, либо о тяжёлой болезни, которые требуют больших финансовых затрат, в связи с чем, просят перевести денежные средства на счет банковской карты.

Перед тем как начать рассылку сообщений, мошенники изучают информацию, имеющуюся на взломанной странице в социальной сети, изучают круг общения. Полученной информацией они пользуются при рассылке сообщений, чтобы их просьба выглядела более убедительно и правдоподобно.

Как реагировать на попытки мошенничества.

- получая тревожные звонки или сообщения, главное – постараться успокоиться и не принимать решения сразу. Скажите звонящему, что Вам необходимо время, чтобы все обдумать, не принимайте поспешных решений;

- никогда и никому не сообщайте свои персональные данные или конфиденциальную информацию банковской карты и счета, логин и пароль от