Принято считать, что жертвами мошенников чаще всего становятся самые социально незащищенные слои населения: инвалиды, пенсионеры.

Однако Центробанк России признал, что в 2019 году наибольшее количество преступлений в сфере электронных платежей совершено в отношении граждан средней возрастной группы.

Многие зачастую не успевают следить за развитием современных технологий: гаджетов, мобильных приложений, чем и пользуются мошенники.

Как правило, мошенники – хорошие психологи. С помощью различных психологических приёмов они с лёгкостью манипулируют людьми, которые до последнего не подозревают, что общаются с преступником.

Для того, чтобы не стать жертвой необходимо при заключении сделок, производстве платежных операций защищать свои данные и не сообщать их третьим лицам без необходимости.

В данном буклете собраны несколько правил, которые помогут вовремя распознать, что Вы имеете дело с мошенником и не позволить ему заполучить Ваши деньги.

Кража, совершённая с банковского счета, а равно в отношении электронных денежных средств,
наказывается штрафом в размере от 100 тыс. до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет, либо принудительными работами на срок до 5 лет с ограничением свободы на срок до 1 года 6 мес. или без такового, либо лишением свободы на срок до 6 лет со штрафом в размере до 80 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 6 мес. либо без такового и с ограничением свободы на срок до 1 г. 6 мес. либо без такового. *(п. «г» ч. 3 ст. 158 УК РФ)*

Мошенничество с использованием электронных средств платежа
наказывается штрафом в размере до 120 тыс. руб или в размере заработной платы или иного дохода осужденного за период до 1 года, либо обязательными работами на срок до 360 ч., либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на срок до 3 лет. *(ч. 1 ст. 159.3 УК РФ)*

Мошенничество в сфере компьютерной информации
то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, наказывается штрафом в размере до 120 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 1 года, либо обязательными работами на срок до 360 ч., либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо арестом на срок до 4 мес. *(ст. 159.6 УК РФ)*

Прокуратура Пермского края

Адрес: 614990, г. Пермь, ул. Луначарского, 60

Телефон доверия: 8(342)217-53-10

Справочная по обращениям: 8(342)217-53-08

ПРОКУРАТУРА ПЕРМСКОГО КРАЯ

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКА

Пермь, 2019

Наиболее частыми видами и способами мошенничества являются:

⇒ предоплата или полная оплата товара на интернет-сайте частных объявлений либо в социальных сетях за товар, который не видели вживую. После перевода денежных средств, продавец, зачастую, перестаёт выходить на связь;

⇒ предоплата или полная оплата брендового товара на интернет-сайте, являющимся подделкой сайта официального производителя, для последующей доставки по почте. Такие мошенники, получив деньги, исчезают вместе с интернет-сайтом в течение нескольких месяцев работы;

⇒ поступление Смс-сообщения с указанием контактного телефонного номера либо звонка якобы от сотрудника банка с информацией о блокировке карты либо о совершении подозрительных операций с банковским счётом. Фактически звонок осуществляется мошенником, который спросит номер карты, CVC-код, а также иные идентифицирующие Вас данные. В дальнейшем, использовав эту информацию, злоумышленник переведёт деньги на свой счёт;

⇒ от незнакомого абонента приходит сообщение о зачислении на ваш мобильный телефон платежа. В дальнейшем, как правило, с этого же номера поступает просьба вернуть ошибочно оплаченные деньги;

⇒ оплата процентов, налогов или доставки предлагаемых несуществующих крупных выигрышей и выгодных кредитов. Такой вид мошенничества, как правило, характерен для социальных сетей;

⇒ звонок от близкого человека с просьбой помочь финансово в целях избежание внезапно возникших проблем (дать взятку сотруднику ГИБДД за сбитого пешехода, оплатить срочную операцию);

⇒ скимминг, то есть считывание при помощи специального устройства данных с магнитной полосы карты.

Как не стать жертвой мошенников при использовании банковской карты и совершении электронных платежей?

• Запишите в телефонную книгу контактные номера родных, близких и коллег, а также телефоны горячих линий банка, чтобы идентифицировать того, кто Вам звонит.

• При звонке с незнакомого номера от имени родственника с просьбой срочно перевести деньги под любым предлогом прервите разговор. Перезвоните тому, от чьего имени обращался звонивший, чтобы узнать, действительно ли ему нужна помощь.

• Если сомневаетесь, что вам позвонил сотрудник банка, попросите его перезвонить через несколько минут. Банковский служащий обязательно совершит повторный звонок, а Вы за это время успеете обратиться на горячую линию банка и узнать, не мошенник ли Вам звонил.

• Не реагируйте на СМС-сообщения с незнакомых номеров.

• Не передавайте Вашу банковскую карту и пароль от нее посторонним лицам.

• Не сообщайте посторонним лицам ваши паспортные данные, реквизиты банковской карты, данные для входа в интернет-банк, а также СМС-сообщения с кодом подтверждения проведения банковских операций.

• Не используйте один пароль для всех Интернет-ресурсов.

• Не совершайте покупки на сайтах, не внушающих доверия.

• Не держите на карте, предназначенной для интернет-покупок, большие суммы.

• Если к Вам поступила информация о победе в розыгрыше, выйдете на связь с его организаторами. Постарайтесь получить от них максимально возможную информацию об акции: условиях участия в ней и правилах ее проведения. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша. Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас.

• При смене номера телефона, к которому подключен мобильный банк, обратитесь в отделение банка с заявлением о прекращении предоставлении услуги по старому номеру телефона.

• При использовании банкомата обратите внимание, исправен ли он, размещена ли информация о владельце банкомата, крепко ли прикреплена клавиатура, а также устройство приёма карт. Некоторые мошенники используют специальных технические приспособления, прикрепляющиеся на банкоматы и позволяющие считать магнитную ленту банковской карты и узнать пин-код.

• Не просите о помощи посторонних в случае возникновения сложностей при снятии денег в банкомате, обратитесь непосредственно к сотрудникам банка.

• Не используйте Вашу банковскую карту, с возможностью Wi-Fi оплаты, на виду у посторонних лиц.

• При утрате банковской карты незамедлительно обратитесь в кредитную организацию (банк), либо на горячую линию банка в целях ее блокировки.

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ С ЗАЯВЛЕНИЕМ В ТЕРРИТОРИАЛЬНЫЙ ОТДЕЛ ПОЛИЦИИ