Мошенничество в сфере использования сотовой сети

Решением комитета Самарской Губернской Думы по транспорту, автомобильным дорогам, информационным технологиям и связи от 18 декабря 2017 №168 утверждены информационные материалы о профилактике правонарушений, совершаемых с использованием мобильных средств связи и в сети Интернет.

Проблема совершения мошенничества в сфере использования сотовой сети сегодня наиболее актуальна. По данным службы Росстат 91 % населения имеет мобильный телефон/смартфон в собственности и, соответственно, пользуется услугами сотовой связи, которая стала инструментом в руках преступников. Самые распространённые преступления, совершаемые с использованием сотовой связи – мошенничество. В результате проведенного опроса российских абонентов установлено, что о мобильном мошенничестве знают 78%, а 15% отметили, что их родственники и друзья пострадали от действий мошенников.

Наиболее распространённые виды мошенничества

1. Мошенничество в сети сотовой связи, связанное с публичным объявлением. Способ обмана прост: на телефон приходит SMS-сообщение о выигранном имуществе и предлагается отправить сообщение, либо позвонить на определенный номер, в результате чего со счета списываются деньги.

2. Звонок на номер абонента с использованием коммерческого номера и моментальный сброс вызова, не дожидаясь ответа. Опасность в том, что может прийти фальшивое сообщение о пополнении баланса, а затем

просьба вернуть эти деньги на указанный номер либо, при перезванивании на номер, списание денег. В любом случае необходимо проявлять бдительность и никому ничего не пересылать.

3. Звонок с сообщением о каком-либо происшествии с родственником, другом абонента либо от лжепредставителей серьезных организаций с просьбой о переводе денег для того, чтобы уладить или оказать помощь близкому человеку абонента. Этот вид мошенничества чаще всего практикуют лица, отбывающие наказание в местах лишения свободы.

4. Хищения, совершаемые с помощью сети Интернет и компьютерной техники. Участились случаи мошенничества в Интернете и связано это с тем, что убеждение человека о том, что он никому не сообщает PIN-код своей карты и не расплачивается ею в местах, которые имеют сомнительную репутацию, – не безоговорочно. Преступления в отношении финансов через Интернет имеют разновидности.

– фишинг: заманивание пользователей на фальшивые сайты и получение доступа к данным платежных карт;

– фарминг: перенаправление жертвы на ложный IP-адрес с целью получения персональных данных клиентов платежных систем;

оба вида мошенничества реализуются без запросов данных, через взлом системы, обманными способами передачи своих данных.Таким образом, человек добровольно передает конфиденциальную информацию третьим лицам;

– вишинг: звонок клиенту от незнакомца, представившегося сотрудником банка. Далее запрос с просьбой ввести номера и PIN-коды своих карт, так как система дала сбой и необходимо обновление

данных. Делают все быстро, не давая возможности для размышлений. Через небольшой промежуток времени деньги с карточек исчезают. Найти мошенников практически невозможно.

– скимминг: мошенничество с помощью устройства «скиммер», которое может перехватывать нужную информацию с магнитных лент на пластиковых карточках. Также есть разновидность скимминга – поддельная клавиатура со встроенной микросхемой, благодаря которой на телефон мошенников приходят СМС-сообщения с PIN-кодами людей.

Как не стать жертвой мошенников и сохранить свои деньги?

1. Пользуйтесь банкоматами, находящимися рядом с банком, где есть камеры видеонаблюдения.

2. Аккуратно храните свои личные данные, никогда и никому их не передавая по электронной почте и тем более по телефону. Серьезные организации не просят у пользователей отправлять или размещать где-либо пароли и ПИН-коды открытым текстом.

Рекомендации гражданам от Роспотребнадзора.

1. Заведите себе электронный кошелек и переводите только те суммы, которые предполагают стоимость покупки. По возможности пользуйтесь лицензионными антивирусными программами на своем ПК.

2. Не вводите свои пароли с чужих компьютеров или гаджетов, не записывайте и не храните пароли офлайн в доступе (спрячьте в надежном месте).

3. При звонках от потенциальных мошенников, несмотря на их угрозы и просьбы не звонить вашему близкому, обязательно перезвоните и проверьте информацию, не

поддавайтесь эмоциям.

4. Рекомендуется настроить SMS-пароли вместо постоянного пароля. Это требует неких усилий, но зато кража пароля фактически исключена, так как он действителен только на один раз!

5. Будьте бдительны, мошенники ежедневно становятся все изобретательнее.