Нововведения в сфере борьбы с интернет-мошенниками

Сегодня в век информационных технологий не только государственное управление, но и современный криминал претерпевает цифровую трансформацию, о чем свидетельствует характер совершаемых преступлений. Преступностью активно применяются новые технологии с целью минимизации объема офлайновых действий при выполнении объективной стороны преступления. Цифровая среда позволяет совершать преступные деяния руками дропперов или других "криминальных аватаров", т.е. людей, которые за денежное вознаграждение либо под воздействием обмана или принуждения, не всегда осознавая свое соучастие в преступлении, выполняют ключевую часть объективной стороны преступления - от незаконного сбыта запрещенных к обороту предметов и дистанционного хищения имущества до поджогов автомобилей, объектов транспортной инфраструктуры и зданий.

Развитие сервисов онлайн-доставки, заказа такси, бронирования жилья, а также онлайн-банкинга и IP-телефонии позволяет совершать дистанционные хищения материальных ценностей.

Подрастающее поколение, находящееся в погоне за высоким заработком, личной финансовой независимостью, к сожалению, все чаще становится «звеном» в преступной «цепи», оказывая содействие преступникам в обналичивании денежных средств, становясь такими же преступниками.

Вопросы противодействия и усиления контроля за деятельностью, связанной с осуществлением банковских операций и переводом денежных средств, остаются актуальными и для законодателя, и для правоприменителя.

Ко второму чтению подготовлен законопроект о противодействии мошенническим схемам по хищению денежных средств граждан с использованием методов социальной инженерии, в результате чего граждане без добровольного согласия принимают на себя кредитные обязательства, попадают под долговую нагрузку и передают деньги злоумышленникам (Проект Федерального закона N 804702-8 "О внесении изменений в отдельные законодательные акты Российской Федерации" (в части создания механизмов противодействия заключению договоров потребительского кредита (займа) и осуществлению операций с использованием денежных средств клиента без его добровольного согласия или с согласия, полученного под влиянием обмана или при злоупотреблении доверием).

Законопроектом предлагаются различные механизмы противодействия осуществлению операций с использованием денежных средств клиента без его согласия или с согласия, полученного под влиянием обмана или при злоупотреблении доверием, включая мероприятия по противодействию заключению договоров потребительского кредита, мероприятия по противодействию операциям по внесению наличных денежных средств на банковские счета с применением токенизированных (цифровых) платежных карт с использованием банкоматов или иных технических устройств, порядок

предоставления квалифицированным бюро кредитных историй сведений для предупреждения возможного мошенничества пользователю кредитной истории, порядок предоставления микрофинансовой организацией заемщику денежных средств по договору потребительского займа, заключенному с использованием сети "Интернет", основания для отказа в заключении договора об использовании электронного средства платежа, порядок проверки сведений о получателе денежных средств, указанных в заявлении о предоставлении потребительского кредита (займа) или распоряжении заемщика о перечислении заемных денежных средств на счет третьего лица, на наличие сведений о получателе денежных средств в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

В этой связи предлагается выработать следующие рекомендации, чтобы снизить риск быть обманутым в сети «Интернет»:

1. Не доверяйте непроверенным сайтам знакомств, заработка, азартных игр, лотерей, тотализаторам.
2. Если на сайте нет юридического адреса, контактных телефонов, обратной связи, то не предоставляйте свои персональные данные, банковские сведения.
3. Не направляйте SMS-сообщения на короткие номера, указанные в инструкции по разблокировке и защите от вирусов.
4. Создавайте сложные пароли там, где есть доступ к Вашим данным и денежным средствам, пользуйтесь обновляемой проверенной антивирусной программой.
5. При совершении покупок в сети «Интернет» предварительно ознакомьтесь с информацией о магазине, отзывами о его работе, инструкцией по возврату и обмену товара. Обратите внимание на дату создания сайта по дате регистрации домена.
6. Будьте аккуратны и внимательны при работе с электронными кошельками и банк-клиентами на сомнительных сайтах, а также при проведении операций на чужих компьютерах.

Проверить данные об организации можно на сайте Федеральной налоговой службы России, используя ИНН и ОГРН. Помимо этого, следует с помощью поиска посмотреть «черный список интернет – магазинов».

Основными признаками того, что Вас пытаются обмануть, являются очень заманчивые и привлекательные предложения, такие как: высокий заработок в «Интернете» за час работы, низкие цены в интернет – магазинах, «легкий» заработок» в виде посредничества при пересылке денежных средств с одного счета на другой, продажа банковских карт.

Нажить много денег – храбрость, сохранить их – мудрость, а умело, в соответствии с нормами действующего законодательства и в рамках правового поля Российской Федерации расходовать – искусство.