

Новые виды и способы совершения мошенничеств

Что такое мошенничество, и на какие виды оно подразделяется по составу преступления, а также количественным и качественным признакам?

В наши дни слово «мошенник» приобретает гораздо более широкий смысл, чем каких-то 20 лет назад, и связано это по большей части с активным развитием интернет-технологий. Так, сегодня можно выделить следующие наиболее распространённые виды мошенничества в уголовной практике:

• Интернет и электронное мошенничество – это наиболее распространённые и сложные способы мошенничества на сегодняшний день, так как злоумышленники практически всегда остаются безнаказанными, а все схемы расставания людей с собственностью и деньгами разрабатываются, прямо сидя у экрана компьютера, например, в случае со знакомствами. Так, мошенники подбирают пароли от электронных кошельков, используя случайные генераторы, крадут пин-коды от банковских карт, а также делают массовые рассылки по электронной почте с предложением поучаствовать в «интересных проектах», но на деле люди, как правило, лишь расстаются со своими деньгами.

Телефонное мошенничество

- Для обмана доверчивых жертв мошенники часто прибегают к преступным схемам предоставления фальшивых документов, как, например, удостоверения правоохранителя, спецслужб, высокопоставленного должностного лица. Входя таким образом в доверие к жертве преступники, как правило, уговаривают жертву отдать определённую сумму денежных средств для решения какой-либо проблемы или в виде оплаты за некачественный товар.

Новинка 2021 года.

В 2021 году Банк России сообщил, что появился новый вид мошенничества. Вернее, вид все тот же, а вот способ... Вам как клиенту какого-то банка звонят на мобильный, представляются сотрудником МВД и объявляют, что против Вас по запросу Банка России возбудили уголовное дело. Ну а дальше пытаются получить у Вас персональные данные, данные банковских карт, сведения об операциях по картам, чтобы потом вывести деньги со счетов. Что делать если получили такой звонок? **Игнорировать**. Банк России выпустил официальное предупреждение, что такие звонки - проделки мошенников. А если Вы все же переживаете, то:

1. спросите у звонящего имя, фамилию и должность;
2. уточните, откуда (из какого отделения) он звонит;
3. перезвоните в это отделение и узнайте, работает ли у них такой сотрудник, попросите соединить.

Важно! Звоните не по тому телефону, который Вам назовет мошенник, а найдя его в официальном источнике, например, на официальном сайте.

Звонок из банка с просьбой связаться со службой безопасности

Вам звонит автоинформатор и сообщает о сомнительных операциях по карте и необходимости перезвонить в банк по номеру (называет). Это не самая избитая схема, многие покупаются на такой прием, поскольку автоинформатор создает ощущение серьезности ситуации.

Что делать? Звонить в банк. Но! **Не на тот номер телефона**, который Вам назвали, а на настоящий, указанный на обороте банковской карты или на официальном сайте банка.

Старый прием со звонком, но с новым звучанием

Вы уже слышали, но я еще раз напомню:

Если Вам звонят якобы из банка, представляются службой безопасности и сообщают о блокировке счета, странных операциях и еще не понятно о чем (насколько хватит фантазии у мошенников), не общайтесь с ними!

А чтобы не переживать за свои деньги, позвоните в банк сами, но надо не перезванивать на номер, с которого звонили, а звонить на официальный номер.

Особенность 2021 года! **Звонить стали девушки, а не мужчины как раньше** (к ним уже все привыкли и наслышаны про тюремные колл-центры). У девушек очень деловой, профессиональный голос. Сразу и не подумаешь, что звонит НЕ сотрудник банка. Будьте бдительны.

Кража данных банковских карт с компьютера

Это не так сложно проверить, поэтому стоит этого опасаться. Ваши логины и пароли к каким-либо сервисам могут украсть с Вашего компьютера, чтобы с их помощью получить данные Ваших банковских карт. Вы ведь оплачиваете что-нибудь картой в Интернете? Чтобы получить логины и пароли, злоумышленники могут взломать Ваш почтовый ящик или подменить сим-карту.

- Достаточно распространены махинации с использованием средств мобильной связи, так как практически каждый гражданин нашей страны владеет собственным номером одного из сотовых операторов. Преобладающее большинство массовых звонков будущим жертвам, равно, как и СМС-сообщений, поступает из мест лишения свободы, где лица, осуждённые за иные преступления, отбывают свои сроки. Так, на номер абонента поступает звонок или текстовое сообщение с привлекательным предложением и просьбой перевода незначительной суммы денег по номеру мобильного телефона или банковской карты. Конечно, люди, оплатившие услуги, ничего взамен не получают.

- Кроме того, мошенники используют очень много преступных схем на транспорте, начиная с оформления в ГИБДД личного автомобиля с просьбой о предоплате услуги через электронный перевод, заканчивая банальным вымогательством денежных средств у населения для нищих, больных и инвалидов. Однако все эти люди на самом деле являются притворщиками, а процесс сбора средств с пассажиров – это лишь прибыльный бизнес. Также многие люди в общественном транспорте сталкиваются с карманными кражами, расчётами наличными с рук с выдачей фальшивой сдачи и т. д.

- Ну и в заключении, конечно, держать ухо востро требуется успешным предпринимателям, так как каждый этап прибыльной деятельности находится под прицелом злоумышленников, начиная от ложных проверок и аудита компании, заканчивая фейковыми конторами по поставке материалов и оборудования, работающими исключительно по предоплате. Данные однодневные юр лица могут иметь собственный интернет-портал, расчётный счёт, десятки положительных отзывов и многие другие регалии, однако это вовсе не значит, что оплаченный товар дойдёт до покупателя, а компанию удастся найти по её юридическому адресу.

Афера на транспорте

Важно! Любая из мошеннических схем, как правило, тщательно продумана до мелочей, и её организаторы являются хорошими психологами, создавая впечатление грамотных специалистов, что вводит жертв в заблуждение, и они легко расстаются с деньгами или предметами собственности.

Так как большинство жертв мошенничества на сегодняшний день встречаются именно в Сети, необходимо подробнее рассмотреть основных схемы обмана пользователей ПК, в частности:

- Фишинг – это новый вид мошенничества, представляющий собой классическую схему внедрения в доверие к жертве с последующим отъёмом у неё денежных средств. Так, рассылка может прийти от крупных банков, например, из «Сбербанка», однако при детальном рассмотрении видно, что адрес отправителя вовсе не содержит в себе хостинговое расширение учреждения. Учреждение требует сделать платёж по кредиту, а доверчивые пользователи начинают противиться этому, так как займов в данном банке у них просто нет. В таких ситуациях «оператор» просит предоставить ему все имеющиеся данные карты или расчётного счёта, включая пароли и пин-коды и в одном случае из 100 все же получает ожидаемый результат.

- Часто пользователям ПК предлагается пройти бесплатную регистрацию на интересном для него портале, после чего отправить бесплатное СМС с подтверждением введённых данных. Как правило, отправка сообщения может стоить 100 руб. и больше, а пользы от контента сайта не будет никакой.

- Достаточно часто в интернете пользователи могут увидеть ссылки на порталы, занимающиеся сбором средств на лечение или поддержку больных детей, инвалидов или малоимущих семей. Однако, если это не официальный портал, зарегистрированный на какой-либо благотворительный фонд, как правило, по ту сторону экрана располагаются мошенники, кладущие все перечисленные на счета средства к себе в карманы. -

Обман в сфере предпринимательства:

- Миллионы интернет-пользователей сталкивались с такой формой мошенничества, как предложения по лёгкому заработку больших денег, но для

того, чтобы принять участие в программе и получить свой персональный аккаунт, будущего бизнесмена просят внести небольшую сумму на номер электронного кошелька, которая, естественно, потом пропадает с концами.

- Интернет-магазины, широко распространённые среди населения сегодня, также далеко не каждый раз предлагают честные способы получения товара. Так, мошенники размещают на своей странице товар с наименьшей ценой, в отличие от других сайтов. Однако чаще всего под товаром стоит приписка – 100% - ная предоплата на банковскую карту. Таким продавцам верить нельзя, и всегда нужно настаивать на оплате товара при получении.

Важно! В связи с участившимся случаем интернет-мошенничества, несколько лет назад на базе МВД РФ был создан специализированный департамент по борьбе с преступлениями, совершёнными в Сети. Так, при написании соответствующего заявления жертва может быть уверена, что бумагу передадут оперативникам именно из этого отдела.