Виртуальные способы мошенничества или преступления с использованием IT-технологии

В современных условиях динамичного развития информационно-телекоммуникационных технологий столь же интенсивно возрастают риски противоправных посягательств в данной сфере.

Мошенничество ‒ одно из самых распространенных преступлений в России. Ежегодно возбуждаются тысячи дел по статье 159 УК РФ. От мошенничества не застрахован никто, ведь злоумышленники постоянно изобретают новые схемы по выманиванию денег. Стать жертвой обмана можно не только в реальной жизни, но и в виртуальном пространстве.

В основном все подобные преступления совершаются с использованием виртуальных абонентских номеров, по которым мошенники представляются сотрудниками служб безопасности банков. Они вводят в заблуждение граждан, вынуждают говорить секретные данные банковских карт и впоследствии похищают денежные средства. В большинстве случаев преступления совершаются с использованием функции подмены абонентского номера, что затрудняет расследование. Гражданам следует помнить – настоящие банковские работники никогда не спрашивают у своих клиентов данные карт и кодов из СМС-сообщений.

Не теряют своей актуальности мошенничества на сайтах бесплатных объявлений, типа «Авито», «Юла» и т.п. Определить настоящего продавца/покупателя от мошенника достаточно просто: продавец просит предоплату, покупатель спрашивает номер карты и код из СМС, вам приходят подозрительные СМС или сообщения в мессенджере, продавец предлагает отправить товар курьерской компанией, продавец или покупатель присылает поддельную ссылку на сервис «Авито Доставка». В подобных случаях с продавцами/покупателями необходимо общаться лично, для мобильных переводов использовать только номер телефона привязанный к карте и ни в коем случае не перечислять предоплату, и никому не сообщать личные данные банковских карт.

Мошенники активно используют в своей преступной деятельности социальные сети: одноклассники, ВКонтакте и другие. Со страниц-двойников рассылаются родным, друзьям, знакомым сообщение о просьбе оказать финансовую помощь, либо подозрительные ссылки, перейдя по которым можно лишиться всех накоплений. Аналогичные СМС могут приходить и в аналоговые сообщения мобильных операторов. Не стоит переходить по неизвестным ссылкам! Если есть желание помочь финансово кому-либо – помогайте адресно, либо через официальные благотворительные фонды.

Большинство преступных схем строится на страсти людей к быстрому обогащению. Например, используя игровые платформы, делая ставки на определённую комбинацию цифр, либо картинок мошенники выручают определённую сумму денег с наивных клиентов, придумывают специальные схемы, а при дальнейшей раскрутке, данная сумма увеличивается. Обязательным требованием подобных игровых платформ – обязательное внесение в выбранное приложение данных банковских карт. И этими данными охотно пользуются мошенники. Различные Интернет приложения, сайты сейчас не обходятся без рекламы. И всплывающие окна с информацией о случайном выигрыше для многих является заманчивой новостью.

Таким образом, в последние годы резко возросло количество преступлений, совершаемых на просторах интернета. К наиболее распространенным можно отнести следующие:

Призыв принять участие во всевозможных конкурсах и проектах. Для участия необходимо перечислить определенную сумму на указанный счет.

Взлом личной страницы. Для возвращения доступа необходимо отправить сообщение на определенный номер, после чего произойдет списание средств, находящихся на счете, а доступ к странице не восстановится.

Блокирование системы вредоносными программами. Схема работает по аналогии с предыдущей. Перечисление денег на лечение детей, открытие приютов для животных и пр.

Рассылка сообщений о блокировании счета в банке. Для разблокировки требуется перейти на указанный сайт и ввести свои личные данные.

Финансовые пирамиды, работающие онлайн.

Продажа каких-либо товаров с внесением предварительной платы. После перечисления денег продавец исчезает или отправляет товар ненадлежащего качества.

Если в Ваш адрес совершены мошеннические действия, обязательно сообщите о факте мошенничества в соответствующие органы. В полицию необходимо обращаться тогда, когда мошеннические действия совершаются физическим лицом. Результат зависит от скорости обращения. Документ можно подать, как лично, так и через интернет-приемную МВД, сайт которой можно найти в интернете.

Если обман совершен юридическим лицом, то на его адрес отправляется письменная претензия, содержащая требование о расторжении договора и возврате средств. А затем подается иск о незаконном обогащении в суд, чтобы начать гражданский процесс.

Простые правила обезопасить себя от мошенников:

Никогда не сообщайте незнакомцам данные банковских карт и коды с СМС-сообщений банков. Помните, настоящим сотрудникам банков они не нужны.

Если назвали мошенникам код или любые другие данные — срочно звоните в банк. Возможно, вы успеете остановить операцию.

Вводите пароли только на тех сайтах, которые открыли сами — например, набрали адрес в браузере.

Если ввели пароль на подозрительном сайте — как можно скорее зайдите на настоящий и смените его.

Включите двухфакторную аутентификацию в почте, социальных сетях и мессенджерах. Тогда кроме логина и пароля потребуется что-то еще: например, код из специального приложения или смс. Мошенники не смогут зайти в ваш аккаунт, даже если украдут или подберут пароль.

Не переходите по ссылкам в сообщениях, даже если сообщение пришло от знакомого. Его аккаунт может быть взломан или продублирован мошенниками.

Запомните: игры, в которые нужно вкладывать реальные денежные средства, на самом деле деньги возвращаются крайне редко.