СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ПРИМЕНЕНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

ОБМАН ПО ТЕЛЕФОНУ. С Вас могут потребовать выкуп или взятку за освобождение якобы из отделения полиции или с места ДТП вашего родственника. Что делать? Главное не паниковать, позвонить самому родственнику, если он не отвечает, то попытаться найти его через родственников или знакомых.

СМС-ПРОСЬБА О ПОМОЩИ. Требование перевести определенную сумму на указанный номер с использованием обращения «мама», «друг», «сынок» и т.п. Что делать? Не спешите переводить деньги, убедитесь, что в них действительно нуждается ваш родственник или знакомый.

ВЫИГРЫШ В ЛОТЕРЕЕ. Вас могут попросить оплатить пошлину, налог и т.п., перевести сумму на определенный счет, сообщить пришедший на телефон код. Что делать? Не спешите переводить деньги или сообщать какие-либо данные по телефону. Позвоните по официальным номерам компании – организатора лотереи или конкурса, указанных на официальных сайтах, убедитесь в том, что вас не обманывают.

ШТРАФНЫЕ САНКЦИИ И УГРОЗА ОТКЛЮЧЕНИЯ НОМЕРА якобы за нарушение договора с оператором вашей мобильной связи. Что делать? Позвоните сами своему оператору по официальному номеру, уточните информацию.

ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ. Вам поступает смс-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок, и мошенник сообщает, что ошибочно перевел деньги на Ваш счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а вы переводите собственные средства. Что делать? Игнорируйте подобные сообщения, если это телефонный разговор, то посоветуйте для возврата ошибочно переведенной суммы обратится в отделение банка.

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

СМС-сообщение о блокировке банковской карты, о несанкционированном движении денежных средств, смене ПИН-кода, окончании срока действия карты и т.д. с требованием перейти по ссылке или перезвонить по указанному телефону.
Телефонный звонок «работника банка», потенциального «покупателя» с предложением пройти к ближайшему банкомату и совершить манипуляции с банковской картой или в мобильном приложении банка во избежание каких-либо последствий, внесении аванса и т.п.

Для сохранности ваших средств соблюдайте основные правила безопасности:
- Никому не сообщайте срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC), пароли и коды из уведомлений, логин и пароль от онлайн-банка.
- Не публикуйте персональные данные в открытом доступе.
- Кодовое слово называйте только сотруднику банка, когда сами звоните на горячую линию.
- Установите антивирусы на все устройства.

МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ

Распространение ссылок на вредоносное программное обеспечение, порнографические сайты, мошеннические ресурсы и приложения. Пользователи социальных сетей часто сталкиваются со спамом. Который приходит к ним в «личные сообщения» от имени «друзей» или незнакомых пользователей. Это означает, что аккаунты этих людей взломаны. Как правило, ссылки в таких сообщениях сопровождаются завлекающим текстом, например: «Видела твои фото, я такого не ожидала, посмотри сам!..», «В этой базе данных есть вся информация на любого человека» и т.п. Что делать? Никогда не переходите по подозрительным ссылкам. Для доступа в социальную сеть используйте уникальный пароль: он должен быть длинным, состоять из цифр и латинских букв. Лучше использовать разные пароли для разных социальных сетей и других интернет-сервисов. Не поддавайтесь на призыв кого-то из «администрации сайта» сообщить ваш логин и пароль под каким-либо предлогом. Регулярно меняйте пароль от социальной сети, остерегайтесь мошеннических сайтов с похожими по написанию названиями (vkontahte.ru, VkOntallke.ru и т.д.). Эти «фишинговые» страницы рассчитаны на невнимательность и на то, что вы сами предоставите мошенникам свой логин и пароль.

Знакомые незнакомцы. В социальных сетях и на сайтах знакомств мошенники создают страницы, где указываются данные и размещаются фотографии вымышленных людей. С помощью этих страниц они знакомятся с другими пользователями сайта. Со временем мошенники входят в доверие, предлагают перейти собеседнику на более «близкое» общение и оставляют свой номер телефона. Самым безобидным последствием такого общения будет то, что номер окажется платным и с вашего счета спишутся деньги.

Просьба о финансовой помощи, благотворительные акции. Мошенники часто используют такие поводы, поэтому, прежде чем перевести деньги для помощи, убедитесь, что вас не обманывают. Обратите внимание на наличие нескольких контактов (телефоны, электронная почта, странички в социальных сетях), наличие подтверждающих документов.

МОШЕННИЧЕСТВО НА САЙТАХ ОБЪЯВЛЕНИЙ

Оплата или предоплата за ваш товар. Очень часто заинтересованные покупатели предлагают произвести оплату или предоплату за ваш товар, но сделать это не могут по каким-либо причинам только на банковскую карту (находится в другом городе, нет наличных денег, деньги на расчетном счету и др.), но при этом требуют сообщить не только номер карты и ФИО (больше для перевода ничего не требуется), но и другие данные. Помните, что если вас просят сообщить пришедший на телефон код, пройти к банкомату и совершить какие-то действия, вставив вашу карту, сообщить срок действия карты и трехзначный код на оборотной стороне, то это мошенники. Прекращайте контакты с такими «покупателями» и, если успели сообщить какие-то данные, немедленно блокируйте банковскую карту.

Предоплата за покупаемый товар. Покупая что-либо, будьте осторожны, если вас просят произвести предоплату. Вполне возможно, что получив ее, «продавец» перестанет отвечать на ваши звонки.

СМС-сообщения со ссылкой. На номер, который вы указали при публикации объявления о продаже или желании что-либо купить, может прийти СМС-сообщение с предложением товара, обмена и ссылкой на этот товар. Если вы перейдете по ссылке, то загрузите на свой телефон вредоносное программное обеспечение, которое позволит мошенникам получить доступ к вашим банковским картам.

Если у вас все-таки украли деньги, то необходимо:
1. Заблокировать карту:
- по номеру телефона банка на банковской карте или на официальном сайте;
- через мобильное приложение;
- через личный кабинет на официальном сайте банка;
- в отделении банка.
2. Написать заявление о несогласии с операцией. Заявление должно быть написано в течении суток после списании денег в отделении банка.
3. Обратиться в полицию.

Подробнее о правилах безопасности читайте на fincult.info

АДМИНИСТРАЦИЯ АЗОВСКОГО РАЙОНА

МЕЖВЕДОМСТВЕННАЯ КОМИССИЯ ПО ПРОФИЛАКТИКЕ ПРАВОНАРУШЕНИЙ В АЗОВСКОМ РАЙОНЕ