ПАМЯТКА

о способах мошенничества с использованием информационно – телекоммуникационных технологий

1. Наиболее простой и распространенный способ совершения преступления IT-преступлений – это оплата покупки товаров и услуг с найденной банковской карты, что в свою очередь, образует собой преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ – кража, совершенная с банковского счёта, а равно в отношении электронных средств платежа, которое наказывается лишением свободы сроком до 6 лет, в связи чем необходимо внимательнее относиться к хранению своих банковских карт и своевременно блокировать в случае утраты, а при обнаружении утраченных банковских карт необходимо воздержать от совершения списаний с них денежных средств.
2. Наиболее общественно опасным способом совершения преступления является введение в заблуждение граждан путем звонка на мобильный телефон с от имени работника банка, сотрудника полиции, прокуратуры, и под предлогом предотвращения совершения в отношении них преступления или необоснованного списания денег с банковской карты предлагается назвать свои персональные данные, реквизиты банковских карт и код СМС-подтверждения, после чего злоумышленники производят списания денежных средств с банковских счетов пострадавшего. В большинстве случаев звонивший обращается к потерпевшему по имени отчеству, чем располагает его к диалогу.

Также, зачастую преступники под различными предлогами просят оформить кредит, обналичит его и перевести на «безопасные счета», «банковские ячейки», которые фактически являются «киви-кошельками», расчетными счетами и банковскими картами, подконтрольные им.
3. Другим распространённым способом совершения преступлений – это перечисление предоплаты преступнику за покупку товара или оказание услуг, информация о которых размещена в сети Интернет, например, на таких сайтах объявлений, социальных сетях или специальных сайтах по продаже какого-либо товара, как привило это автозапчасти, компетентная техника, средства связи и животные. После перечисления предоплаты лицо, её получившее, на связь с покупателем не выходит и свои обязательства

не исполняет.

Другой разновидностью указанного способа мошенничества является приобретение товара в Интернете и оплата его путем перечисления наложенного платежа. Зачастую, после получения почтового отправления в нем обнаруживается дешевый и некачественный аналог заказанного товара.

4. В последнее время участились случаи, когда злоумышленники введя в заблуждение граждан, в ходе телефонного разговора, опять же представляясь сотрудником банка, убеждают установить на используемое потерпевшим устройство дополнительное приложение удаленного управления, которое является отражением мобильного телефона потерпевшего, после чего удаленным способом, уже получив доступ к мобильному приложению банка совершают хищение денежных средств с банковского счета потерпевшего.

5. Остается в настоящее время способ совершения мошеннических действий, когда злоумышленники осуществляют звонок потерпевшему, выдавая себя за их родственника и просят оказать финансовую помощь чтобы избежать ответственности за совершение того или иного правонарушения (совершили ДТП или подрались, в результате чего пострадали люди и чтобы не нести уголовную ответственности необходимо компенсировать причиненный вред).

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!!

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА

«ОНЛАЙН ПОКУПКИ»
Якобы продавец просит за товар предоплату либо полную оплату покупки, после чего связь с мошенником прекращается

«МЫ НАШЛИ ВАШИ ДОКУМЕНТЫ»
Якобы нашли ваши утерянные документы и просят вознаграждение за их возврат

«ПРИВЯЗКА КАРТЫ»
Просят привязать вашу банковскую карту к какому-либо номеру телефона или счету

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВЫПЛАТА ПРОЦЕНТОВ»
Обещание больших процентов по вкладам под короткие сроки на различных интернет сайтах

«ПОКУПКА АВИАБИЛЕТОВ»
продажа липовых авиабилетов на мошеннических сайтах

ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ

Помните! Ни в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счету ни под каким предлогом!
Пользуйтесь только проверенными сайтами, на которых решили совершить какие-либо покупки!
Оплачивайте товар только после его получения!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«ВАША КАРТА ЗАБЛОКИРОВАНА»
SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»
Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»
SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»
Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»
просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Помните! Если вам звонят и тревожным голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники!
Никогда не проходите по ссылкам присланный в SMS-сообщении с незнакомых номеров!
Никому не сообщайте ПИН-код вашей банковской карты!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!