Основные способы совершения хищений в сфере ИТТ

1. Звонки из CALL-центров:

- аннулирование кредита, предотвращение несанкционированного списания, пролонгация срока действия договора на оказание услуг связи - получают коды из СМС, позволяющие осуществить вход в личный кабинет онлайн банкинга потерпевшего и совершить манипуляции по переводу средств (оформить кредит), а также доступ к ГОСУСЛУГам и иным сервисам.

- звонки от имени спец служб (ФСБ, МВД, следственный комитет) – под предлогом участия в спецоперации по вычислению недобросовестных работников банковского сектора.

- сохранение денежных средств на т.н. «резервном или безопасном» счете.

- использование «фейкового» аккаунта мессенджера руководителя работодателя.

(***резервных счетов не существует***).

2. Использование интернет ресурсов по размещению бесплатных объявлений и оказания услуг пассажироперевозок (**АВИТО, Юла, БЛАБЛАКАР**), а также сервисов знакомств (**МАМБА, Вконтакте**):

- в процессе товарно-денежных отношений просят перевести денежные средств (задаток),

- просят перейти в мессенджеры для упрощения общения, где в последующем отправляют ссылку для оплаты либо доставки товара, тем самым потерпевший попадает на фейковый сайт платежных систем и вводит данные банковской карты **(№ банковской карты, CVC, СМС).**

- под предлогом знакомства и приобретения билетов в театр, также посредством использования «фейковых» сайтов.

(*данные сайты администрируются на зарубежных хостингах, в том числе США, КЛАУДФЛЭЙР).*

Торговые площадки оснащены системой защиты от сомнительных операций по переводу средств, позволяющей блокировать различные ссылки, поэтому если Вас покупатель/продавец просит перейти к общению в мессенджере и кидает ссылку, то это первый тревожный сигнал к тому, что Вас хотят обмануть. Зачастую ссылки, отправляемые преступниками, по названию могут быть схожи с названиями различных компаний по доставкам товара, даже с названиями самих торговых площадок. Не переходите по ссылкам, отправленным неизвестными лицами**).**

3. Биржи, под предлогом инвестирования средств. Потерпевшим предлагается установить программы для игры на бирже, перейти на фейковые сайты, где наглядно отображается имитация получения прибыли. Итог один – потеря вложенных средств.

4. Дополнительный заработок на маркетплейсах. В целях повышения рейтинга товара на торговых площадках потерпевшему предлагается ставить ЛАЙКИ, за каждый ЛАЙК выплачивается определенная сумма, после чего предлагается оплатить стоимость товара, вначале сумма возвращается потерпевшему в увеличенном размере. Как только потерпевший заказывает и оплачивает товар на значительную сумму, злоумышленники исчезают.

Иные распространенные способы:

1. «Родственник в беде, совершил ДТП»;

2. Оформление микрокредита в микрофинансовой организации;

3. Просьба одолжить деньги через мессенджеры, социальные сети;

4. Помощь в трудной жизненной ситуации (болезнь, похороны и т.п.);

5. Помощь в возврате утерянных вещей, предметов, документов и т.д. за вознаграждение;

6. Компенсация за БАДы, иные гос. выплаты, выигрыш в лотерею;

7. Доставка продуктов, вещей, товаров;

8. Сайты знакомств (вымогательства за интим. фото и т.д.);

9. Заказ такси, услуга по доставке цветов, сопровождающиеся просьбой пополнить баланс телефона.

УБК УМВД России по Оренбургской области