Алгоритм действий для органов местного самоуправления и работодателей для проведения разъяснительной работы по профилактике преступлений, связанных с дистанционными хищениями денежных средств с гражданами и трудовыми коллективами

Провести разъяснительную работу по тематике «Как не стать жертвой мошенничеств и иных преступлений, связанных с дистанционными хищениями денежных средств», довести наиболее распространенные схемы совершения указанных преступлений:

<u>«Звонок службы безопасности банка»</u>

В процессе телефонного звонка потерпевшему сообщаются сведения о том, что по его банковской карте проводятся подозрительные операции. Для спасения денежных средств мошенники просят перевести деньги на «защищенные счета» (ими выступают подконтрольные злоумышленнику номера сотовых телефонов или банковские карты). Либо под предлогом отмены операции потерпевший устанавливает приложение «Team Viever Quick Support», позволяющее удаленным способом управлять устройством, в результате чего у потерпевшего списываются денежные средства.

Также имеют место факты, когда помимо хищения хранящихся на банковской карте денежных средств, злоумышленники удаленным способом оформляют кредит в банке или принуждают потерпевшего его оформить путем посещения ближайшего офиса банка, а потом похищают денежные средства. Потерпевший при этом снимает все хранящиеся на счетах деньги, берет кредиты (чтобы не получили на его имя другие лица) и переводит деньги на защищенные ячейки (номера телефонов). Либо злоумышленники просят потерпевшего установить приложение «Мир рау» и привязать к нему банковскую карту злоумышленника (физическая карта в пластике у мошенника, а у потерпевшего электронный образ). При пополнении карты потерпевший полагает, что деньги защищены, т.к. карта привязана к его телефону, а деньги снимаются злоумышленниками с физического пластика.

Рекомендуется: Прекратить общение, в целях проверки информации обратиться в банк и в полицию, не предпринимать активных действий «по спасению денег».

«Продажа товара или оказание услуг через сайт бесплатных объявлений»

В процессе переговоров злоумышленник получает предоплату за товар или услуги, после чего удаляет учетную запись, а товар не поставляет, услуги не оказываются. Либо в процессе переговоров узнает у продавца реквизиты банковской карты покупателя якобы для перевода денежных средств и похищает хранящиеся на банковской карте деньги.

Рекомендуется: Ознакомиться с правилами пользования сайта, не переходить по сторонним ссылкам из защищенных чатов, помнить, что CVV код (три цифры на обратной стороне необходим исключительно для списания денежных средств), для покупок в сети интернет использовать отдельную банковскую карту.

«Продажа товара в сети Интернет»

Сайт внешне схож с интернет-магазином крупной кампании или просто качественно сделан и внушает доверие, цены как правило ниже среднерыночных. После перевода денег продавец пропадает, сайт через некоторое время закрывается, товар не отгружается.

Рекомендуется: Перед осуществлением перевода денежных средств необходимо ознакомиться с отзывами о продавце, с большой осторожностью относиться к недавно созданным магазинам. Пользоваться сервисами по анализу цены и наличию товара в проверенных магазинах (яндекс поиск товаров и т.д.).

«Помощь родственнику или знакомому»

В социальной сети в «Вконтакте» с взломанного (находящегося под контролем злоумышленника) или внешне схожего аккаунта родственника или знакомого приходит сообщение о том, что возникли финансовые сложности и необходимо перечислить денежные средства на банковскую карту ПАО «ВТБ» (как правило на самом деле ПАО «Почта банка» или «Киви банк»). После перечисления денежных средств на счет, связь прерывается (происходит всплесками, при попадании базы со слитыми паролями к учетным записям пользователей социальных сетей).

Рекомендуется: Включить двухфакторную аутентификация (чтобы приходил код на телефон) и осуществлять смену пароля не реже чем раз в 3-6 месяцев. Перед переводом денежных средств уточнять такую необходимость либо личным звонком, либо проверить личность обратившегося «вопросом – ловушкой».

<u>«Помощь родственнику попавшему в ДТП»</u>

Как правило звонок поступает на городской номер телефона, злоумышленник сразу говорит: «Мама, это я». Поняв, что потерпевший узнал голос одного из родственников, мошенник сообщает что попал в ДТП и необходимо срочно передать крупную сумму денежных средств. При этом злоумышленник якобы передает телефон сотруднику полиции, который вводит пожилого человека в стрессовое состояние сообщениями о жертвах и уголовном преследовании.

Рекомендуется: Связаться с родственником по ранее известным телефонам. Если нет такой возможности проконсультироваться с соседями, друзьями, не предпринимать действий по отчуждению денег.

<u>Дополнительный заработок в сети интернет» или «инвестиции денежных средств», биржа</u>

Злоумышленник размещает на различных интернет-платформах либо путем обзвона граждан сообщает информацию о возможности участия в инвестиционной деятельности. При этом изначально злоумышленник использует приманку, предлагая удвоить сумму вложенных им денежных средств в течение суток, что и происходит: гражданин в этот же день получает двойной заработок. Далее злоумышленник, продолжая реализацию преступного умысла, убеждает гражданина вносить крупные суммы денежных средств. Для убедительности гражданину предлагается установить приложение для отслеживания денежных средств и роста прибыли. Требование гражданина о выводе денежных средств злоумышленник не выполняет, получая денежные средства.

Рекомендуется: Не принимать участие в инвестиционной деятельности на интернет-платформах, либо пользоваться заранее проверенными.

Хищение, совершенное с использованием вредоносных программ на ОС «Android»

Потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом: «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка: www.avit.o/ru/FriZsk», или SMS-сообщение с текстом: «Смотри как мы получились на этой фотографии. Ссылка: www.avit.o/ru/FriZskAa». Потерпевший проходит по данной ссылке, в результате чего загружает на свой телефон вирус, предоставляющий мошеннику доступ к SMS-командам. В дальнейшем мошенник похищает деньги, путем направления SMS-сообщений на номер «900».

Рекомендуется: Не использовать сомнительные ссылки в SMS-сообщениях.

УМВД России по Вологодской области