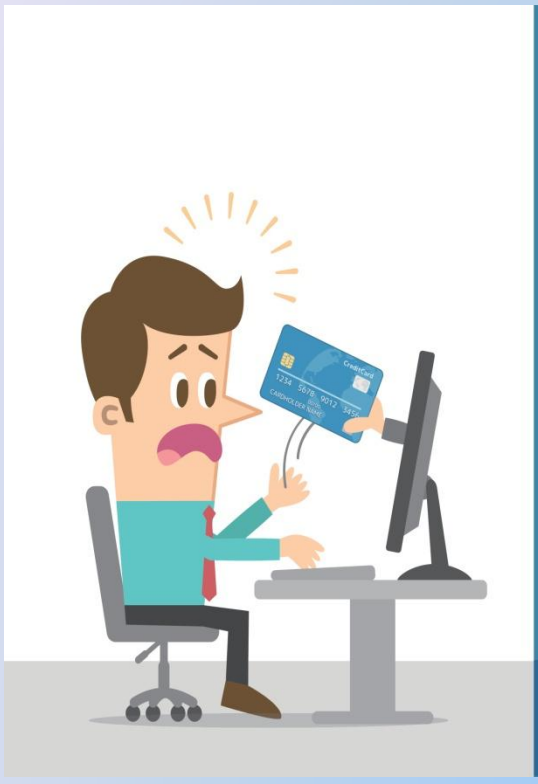
МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ



Наиболее распространённые способы совершения преступления

МОШЕННИЧЕСТВО НА «АВИТО» И ДРУГИХ САЙТАХ

СЫН/РОДСТВЕННИК ПОПАЛ В ПОЛИЦИЮ; СМС ИЛИ ЗВОНОК «ВАША КАРТА ЗАБЛОКИРОВАНА..»

ПОД ВИДОМ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ИЛИ ПРЕДСТАВИТЕЛЯМИ АДМИНИСТРАЦИИ ГОРОДСКИХ ОКРУГОВ

ВЫМОГАТЕЛЬСТВО, МОШЕННИЧЕСТВО И КРАЖИ ДЕНЕЖНЫХ СРЕДСТВ В ОТНОШЕНИИ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

МОШЕННИЧЕСТВО НА «АВИТО» И ДРУГИХ САЙТАХ

1

- после согласования всех условий покупки товара и перевода денежных средств, в конечном итоге товар не поставляется покупателю

- Создание различных интернет –магазинов По продаже популярных среди населения товаров, по ценам значительно ниже рыночных. Потерпевший переводит денежные средства , однако в установленные сроки товар не доставляется покупателю, а продавец не выходит на связь.

Признаки мошенничества со стороны продавца

Отсутствует адрес и телефон, все общение предлагается вести через электронную почту или соц. сети

Отсутствует реальное имя продавца, человек скрывается под «ником»

Продавец принимает оплату только на анонимные реквизиты

Объявление составлено с ошибками, с использованием транслитерации, без знаков препинания и т.д

Продавец зарегистрирован недавно, объявление о продаже – единственное его сообщение

Слишком низкая цена товара в сравнении с аналогами у других продавцов

Продавец требует полную или частичную предоплату

Признаки мошенничества со стороны покупателя

ПОКУПАТЕЛЬ НЕ ОСОБО ИНТЕРЕСУЕТСЯ ТОВАРОМ, БЫСТРО ДЕМОНСТРИРУЕТ СВОЕ ЖЕЛАНИЕ СДЕЛАТЬ ПОКУПКУ И ПЕРЕХОДИТ К РАЗГОВОРУ О СПОСОБЕ ПЛАТЫ

ПОКУПАТЕЛЬ ПРОСИТ ВАС СООБЩИТЬ ЕМУ РАЗЛИЧНЫЕ КОДЫ, КОТОРЫЕ ПРИДУТ К ВАМ НА МОБИЛЬНЫЙ ТЕЛЕФОН, ЯКОБЫ НЕОБХОДИМЫЕ ЕМУ ДЛЯ СОВЕРШЕНИЯ ПЛАТЕЖА

ПОКУПАТЕЛЬ ПРОСИТ ВАС НАЗВАТЬ ПОЛНЫЕ РЕКВИЗИТЫ КАРТЫ, ВКЛЮЧАЯ ФАМИЛИЮ-ИМЯ ЛАТИНИЦЕЙ, СРОК ДЕЙСТВИЯ И CVC – КОД. ПРИ ПОМОЩИ ЭТИХ ДАННЫХ ОН САМ ЛЕГКО СМОЖЕТ РАСПЛАТИТЬСЯ ВАШЕЙ КАРТОЙ В ИНТЕРНЕТЕ

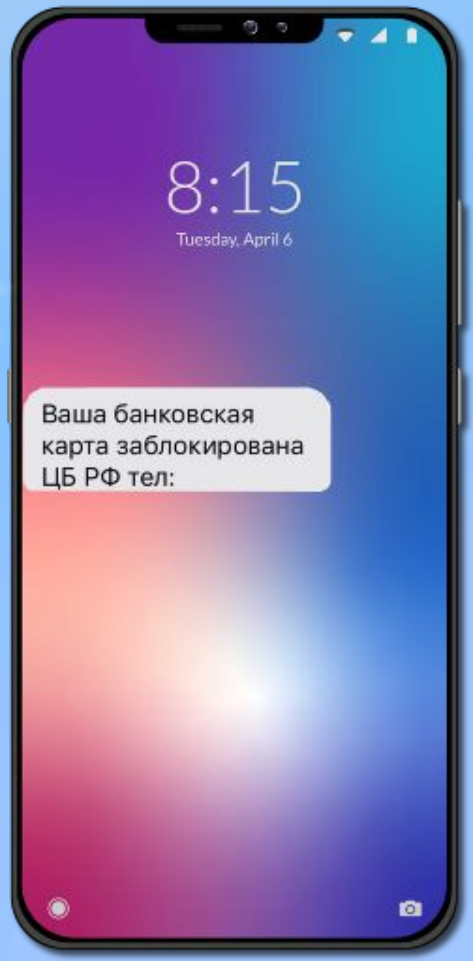
КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИСЧЕСТВА

- *Следует внимательно изучить информацию Интернет-сайта, отзывы, сравнить цены за интересующий товар. Отсутствие информации, запутанная система получения товара, зачастую является признаками мошенничества.*
- *Нельзя сообщать информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести различные покупки.*
- *Получить максимум сведений о продавце или магазине, адреса, телефона, наличие службы доставки и т.д. Действующие легально Интернет - магазины размещают полную информацию и работают по принципу «оплата товара после доставки»*

Сын/родственник попал в полицию; СМС или звонок «Ваша карта заблокирована»

2

ПРЕСТУПНИКИ ЗВОНЯТ ГРАЖДАНАМ ПОД ВИДОМ РАБОТНИКОВ БАНКОВСКИХ СТРУКТУР С ЦЕЛЬЮ ПРЕДУПРЕЖДЕНИЯ ФАКТОВ КРАЖ, И В ХОДЕ ТЕЛЕФОННЫХ БЕСЕД УБЕЖДАЮТ ГРАЖДАН ИЛИ ПЕРЕДАТЬ РЕКВИЗИТЫ УПРАВЛЕНИЯ СЧЕТАМИ ИЛИ ПЕРЕВЕСТИ ДЕНЕЖНЫЕ СРЕДСТВА НА БЕЗОПАСНЫЕ СЧЕТА, ПРИ ЭТОМ ИСПОЛЬЗУЕТСЯ IP – ТЕЛЕФОНИЯ, ВОЗМОЖНОСТИ КОТОРОЙ ПОЗВОЛЯЮТ СОВЕРШАТЬ ЗВОНКИ ВЛАДЕЛЬЦАМ БАНКОВСКИХ КАРТ ОТ ИМЕНИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКОВ, С ТЕЛЕФОННЫХ НОМЕРОВ ИДЕНТИЧНЫХ НОМЕРАМ БАНКОВСКИХ ОРГАНИЗАЦИЙ



Под видом сотрудников правоохранительных органов или представителями администрации городских округов

3

В ДАННОМ СЛУЧАЕ ЗЛОУМЫШЛЕННИК, ЗАРАНЕЕ УЗНАВ В СЕТИ ИНТЕРНЕТ АДРЕС И ДОЛЖНОСТНЫХ ЛИЦ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ОСУЩЕСТВЛЯЕТ ЗВОНКИ В МАГАЗИНЫ, ОСУЩЕСТВЛЯЮЩИХ ДОСТАВКУ ПРИОБРЕТАЕМЫХ ТОВАРОВ.

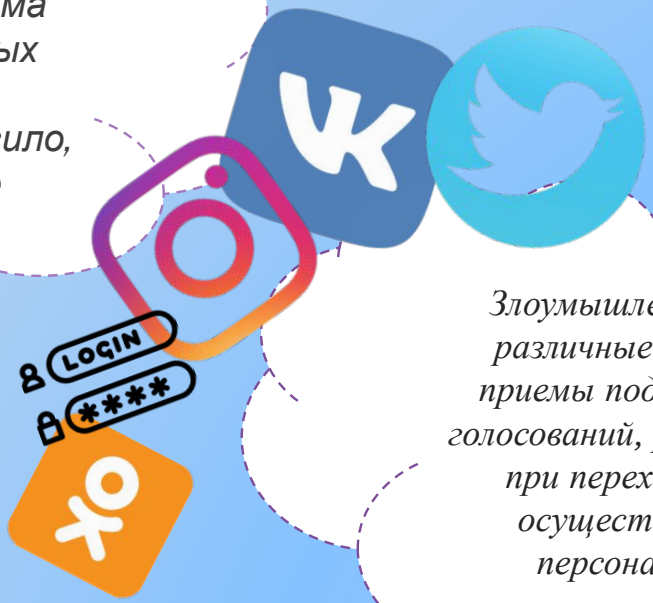
ВО ВРЕМЯ ОСУЩЕСТВЛЕНИЯ ДОСТАВКИ, ЗЛОУМЫШЛЕННИК ПРОСИТ ПЕРЕВЕСТИ ДЕНЕЖНЫЕ СРЕДСТВА ПОД РАЗЛИЧНЫМИ ПРЕДЛОГАМИ НА АБОНЕНТСКИЕ НОМЕРА.

ОДНАКО, ПОЛУЧИВ ДЕНЕЖНЫЕ СРЕДСТВА ОТ ПОТЕРПЕВШЕГО, СВЯЗЬ С ЗЛОУМЫШЛЕННИКОМ ПРОПАДАЕТ.

Вымогательство, мошенничество и кражи денежных средств в отношении пользователей социальных сетей.

4

Остается острая проблема сохранности персональных данных в различных социальных сетях, как правило, в соц.сети ***ВКонтакте***



Злоумышленники, используя различные психологические приемы под видом различных голосований, рассылают ссылки, при переходе по которой осуществляется кража персональных данных

Помните!

- *Ни в коем случае не сообщайте КОДЫ и ПАРОЛИ подтверждения операции, приходящие в смс – сообщениях;*
- *Не сообщайте номер вашей банковской карты вместе с CUV-кодом;*
- *Не вступайте в беседы с незнакомцами, которые звонят с неизвестных вам номеров;*
- *Ни в коем случае не переводите денежные средства на какие-либо счета и тем более абонентские номера;*
- *Устанавливайте сложные пароли доступа к персональной странице, устанавливая двойную аутентификацию.*