Мошенничество с использованием «СОТОВОЙ СВЯЗИ»

Мошенничество с использованием средств сотовой связи, как правило, совершается путем сообщения гражданам **следующей заведомо ложной информации:**

-сообщение о попадании близкого в ДТП или совершении им преступления, после чего следует требование о необходимости перевода или передачи денежных средств

-поступление звонка или СМС-сообщения от «сотрудников службы безопасности банка», после чего следует сообщение о блокировке карт, аресте счетов, незаконном списании денежных средств и необходимости сообщить реквизиты карты и иные данные

-получение звонка или СМС-сообщения о том, что вы стали обладателем приза или победителем конкурса, после чего следует просьба о перечислении денежных средств как гарантии получения выигрыша

Как не стать жертвой мошенничества с использованием сотовой связи?

Позвоните своему близкому человеку, в учреждение здравоохранения, правоохранительные органы с целью проверки информации, поступившей в ходе телефонного звонка или СМС-сообщения

НИКОГДА *не передавайте и не переводите деньги незнакомым людям*

Прокуратура Березовского района Пермского края

«Мошенничество с использованием информационно-телекоммуникационных технологий»

с. Березовка Пермский край

2024

«КИБЕРМОШЕННИЧЕСТВО»

Хищение денежных средств в следующих случаях:

-на Ваш смартфон или компьютер поступает сообщение, либо письмо с любой информацией которая способна Вас заинтересовать, в котором содержится ссылка, по которой необходимо перейти

-самостоятельная установка нелицензионного программного обеспечения с предоставлением доступа к сети «Интернет, отправке СМС-сообщений

-утеря мобильного телефона с подключенной услугой «Мобильный банк»

Как не стать жертвой кибермошенничества?

-не переходите по ссылкам и не устанавливайте приложения / обновления, направленные по СМС, ММС, электронной почте, мессенджерам, в том числе, от имени банка

-в случае утери мобильного телефона с услугой «Мобильный банк» следует немедленно обратиться в контактный центр банка для блокировки услуги

МОШЕННИЧЕСТВО В СЕТИ «ИНТЕРНЕТ»

Мошенничество при покупках или продажах через сеть «Интернет» (онлайн-магазины, социальные сети, ресурсы объявлений).

Способы:

-создание «сайтов – клонов» известных торговых площадок (копирование интерфейса оригинального сайта) с небольшим отличием в доменном имени сайта, с использованием которых осуществляется ложная продажа товара

-размещение от Вашего имени в сети «Интернет» объявления о продаже товара, после чего Вам звонит потенциальный покупатель и заявляет о намерении приобрести товар и просит сообщить данные Вашей банковской карты для перевода денежных средств

Как не стать жертвой мошенничества в сети «Интернет»?

-осуществление проверки правильности написания доменного имени сайта

-проверка контактных данных сайта, где осуществляется продажа товаров (если указан лишь адрес электронной почты или телефон рекомендуется воздержаться от покупки)

-никому не сообщайте данные своей банковской карты